



POLICY ON KNOW YOUR CUSTOMER AND ANTI- MONEY LAUNDERING MEASURES

Version Control:

Name of Policy	Version	Board approval date	Remarks
Policy on Know Your Customer and Anti-Money Laundering Measures	V1.0	December 1, 2023	Policy document approved.
Policy on Know Your Customer and Anti-Money Laundering Measures	V2.0	May 26, 2025	Policy document revised.

CHAPTER -I

1) Introduction:

Reserve Bank of India has issued Master Direction- Know Your Customer (KYC) Direction, 2023 including comprehensive guidelines on Know Your Customer (KYC) norms and Anti-money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company.

This policy is applicable to all categories of products and services offered by the Company.

2) Definitions:

- i. **“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.
- ii. **“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.
- iii. **“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.
- iv. **“CKYC Identifier”**: Upon successful submission/registration of KYC Documents of the Borrower on CERSAI Portal, a 14- digit KYC Identifier Number (KIN) is issued. An SMS/email will be sent to the Borrower, once the KIN is generated. The Company need to ensure that the KIN is communicated to the Customer (either individual/Legal Entity) as the case may be.
- v. **“Certified Copy” (Original Seen & Verified/OSV)** - Obtaining a certified copy or OSV 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.

vi. Customer

For the purpose of KYC Guidelines, a "customer" is defined as:

1. A person or entity that maintains an account and/or has a business relationship with the Company including customers associated with the selling/marketing of permitted insurance business of the NBFC.
2. One on whose behalf the account is maintained (i.e. the beneficial owner);
3. Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Company Secretaries, Chartered Accountants, Solicitors etc. as permitted under the law, and
4. Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company, say a wire transfer or issue of a high value demand draft as a single transaction.

vii. "Customer Due Diligence (CDD)" means **identifying and verifying** the customer and the beneficial owner.

viii. "Customer identification" means undertaking the process of CDD.

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.

xi. "FATCA" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S Tax payers or foreign entities in which U.S Tax payers hold a substantial ownership interest.

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

xiii. "Non-face-to-face customers" means customers who open accounts without visiting the branch/ offices of the company or meeting the officials/ authorized representatives of the Company.

- xiv. "Offline verification"**
Means the process of verifying the identity of the **Aadhaar number holder** without authentication, through such offline modes as may be specified by regulations.
- xv. "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.
- xvi. "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.
- xvii. "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/military officers, senior executives of state-owned corporations, important political party officials, etc.
- xviii. "Principal Officer"** means an officer nominated by the Company, responsible for furnishing information as per rule 8 of the Rules.

CHAPTER -II

3) CUSTOMER ACCEPTANCE POLICY:

The Company shall follow the following norms while accepting and dealing with its customers:

1. No account is opened in anonymous or fictitious / benami name.
2. No account is opened where the RE is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The RE shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD.
3. No transaction or account-based relationship is undertaken without following the CDD procedure No transaction or account-based relationship is undertaken without following the CDD procedure.
4. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
5. Additional information, where such information requirement has not been specified in the internal KYC Policy of the RE, is obtained with the explicit consent of the customer.

6. REs shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a RE desires to open another account with the same RE, there shall be no need for a fresh CDD exercise.
7. CDD Procedure is followed for all the joint account holders, while opening a joint account.
8. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
9. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of this MD.
10. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
11. Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000.
12. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

4) CUSTOMER IDENTIFICATION PROCEDURE:

- I. The Company shall undertake identification of customers before commencement of an account based relationship. Customer identification means identifying the customer and verifying his / her identity by using reliable and independent source of documents, data or information to ensure that the customer is not a fictitious/ anonymous/ benami person. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business relationship.
- II. An effective Customer Identification Program ("CIP") is an important part of the effort by the Company to know its customers. The Company's CIP is integrated into the AML (Anti Money Laundering) program for the company in terms of the Prevention of Money Laundering Act, 2002 and the relevant rules notified there under (PMLA), which contains provisions requiring the business processes to:
 - **Verify the identity of any Person** transacting with the Company to the extent reasonable and practicable

- **Maintain records of the information** used to verify a customer's identity, including name, address and other identifying information and
- Consult sanctions lists/ FATF statements of known or suspected terrorists: The Company shall ensure that, in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, -the Company does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved and periodically circulated by the United Nations Security Council (UNSC) and whose names appear in the sanctions lists circulated by Reserve Bank of India. The Company may ensure the aforesaid, verifying the name of person or entity through the website of the concerned entity or through the service provider, who provide the said service of third party verification, in compliance applicable provisions/guideline of Reserve Bank of India/National Housing Bank, the Prevention of Money Laundering Act and rules made thereunder in this regard.
- Details of accounts/ customers bearing resemblance with any of the individuals/entities in the list, shall be treated as suspicious and reported to the FIU-IND, apart from advising Ministry of Home Affairs as required under UAPA notification.
- The Credit Head, will be responsible to ensure that, the name of Borrower is not reflecting in the aforesaid list.
- The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

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

- a. Commencement of an account-based relationship with the customer.
- b. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
- c. Selling third party products as agent.

IV. The Company shall take reasonable measures to ascertain and verify the true identity of all customers who transact with the Company. Each business process

shall design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers and the associated risks. Such standards and procedures shall include, at a minimum, the following elements.

V. IDENTIFICATION:

All the customers shall be identified by a unique identification code to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers.

The customer identification requirement is detailed in **Annexure- II** to this policy. Each business process shall implement procedures to obtain from each Customer, prior to transacting, the following information as may be relevant, to that business:

- a) **Name:** procedures require business processes to use reasonable efforts to ensure that the name recorded on the Company systems as the customer will be exactly the same as (and not merely similar to, or a variation of) the name that appears on any identifying documentation reviewed in connection with the loan;
- b) **For individuals - age / date of birth;** For a person other than individual (such as corporation, partnership or trust) - date of incorporation;
- c) Address including the documentary proof thereof:
 - i. For an individual, a residential or business street address;
 - ii. For a Person other than an individual (such as a corporation, partnership, or trust), the principal place of business, local office, or other physical location;
- d) Telephone/Fax number/E-mail ID;
- e) **Identification number:**
 - i) A taxpayer identification number; passport number and country of issuance; proof of possession of Aadhaar number; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard or the unique number or code assigned by the Central KYC Records Registry. When opening an account for a person (other than an individual) that does not have an identification number, the business process must request alternative government-issued documentation certifying the existence of the business or enterprise;

Where a customer submits proof of possession of Aadhaar number, the Company shall ensure that such customer redacts or blackout his Aadhaar number before submitting the same to the Company.

The submission of Aadhaar is mandatory only when the customer is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act or as per the Notification, Circular, Guidelines, as may be issued by RBI read with Directions/Guidelines, issued UIDAI from time to time, otherwise Aadhaar is not mandatory and the Company not to insist for the same. However,

the individual, if so desires, may provide the same out of volition. The customer, at their option, shall submit one of the OVDs.

- ii) For a customer who has applied for, but has not received an identification number, loan may be sanctioned, but each business process shall implement procedures to confirm that the application was filed before the loan is sanctioned to customer and to obtain the identification number within a reasonable period of time before disbursement of loan.

- f) **One recent photograph of the individual customer.** Fresh photographs will be obtained from minor customer on becoming major.

For undertaking CDD, the list of documents that can be accepted as proof of identity and address from various customers across various products offered by the Company is given as **Annexure- III** to this policy. These are appropriately covered in the credit policies of the respective businesses and communicated to the credit approving authorities.

5) CUSTOMER DUE DILIGENCE (CDD)/VERIFICATION:

Each business process as a part of the credit policy will document and implement appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the true identity of its customers. Verification of customer identity should occur before transacting with the customer. Procedures for each business process shall describe acceptable methods of verification of customer identity, which may include verification through documents or non-documentary verification methods that are appropriate given the nature of the business process, the products and services provided and the associated risks.

I. Verification through Officially Valid Documents:

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.

These documents may include, but are not limited to the list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company as provided in **Annexure - III** to this policy. These are appropriately covered in the credit policies of the respective businesses. The customer verification processes will be covered in detail in the credit policies of every business.

II. Verification through Non-Documentary Methods:

These methods may include, but are not limited to:

- i. Contacting or visiting a customer;
- ii. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
- iii. Checking references with other financial institutions; or
- iv. Obtaining a financial statement.

III. Offline Verification:

The Company may carry out offline verification of a customer under the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016, Directions/Guidelines issued by the Unique Identification Authority of India (hereinafter referred as Aadhaar Regulations) if the customer is desirous of undergoing Aadhaar offline verification for identification purpose.

Offline Verification can be done by following two ways:

Option 1: Using the Quick Response (QR) codes:

Seek the Aadhaar QR code from the customers. The same has to be download and printed by the customer and submitted to the company who shall read it using a QR code reader. Scanning of QR code, from the QR code reader will provide the name, address and photograph of the customer, without providing the Aadhaar number.

Option 2: Using paperless local e-KYC:

The paperless local e-KYC involves generation of a digitally signed XML which can be stored in a laptop or phone and be communicated by the customer to the company, as and when required. Companies can receive the Aadhaar Paperless Offline e-KYC XML from the customers. The XML file provides the name, address and photograph of the customer, without providing the Aadhaar number.

No such offline verification will be performed without obtaining the written consent of the customer in the manner prescribed in the Notification, Circular and Guideline issued by RBI read with Aadhaar Regulations.

Except in accordance with the Notification, Circular, Guidelines issued by RBI read with Aadhaar Regulations, the Company shall not collect, use or store an Aadhaar number of its customer for any purpose.

IV. Verification of equivalent e-document:

Where the customer submits an equivalent e-document of any Officially Valid Document (OVD), issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and take live photo of the customer as specified under digital KYC in RBI regulations.

V. Verification based on Digital KYC:

QGO can undertake the Digital KYC process for CDD in which live photo of the customer will be captured and officially valid document or the proof of possession of Aadhaar to be taken, 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 QGO, as per the provisions contained in the Prevention of Money Laundering Act, 2002 and the rules made thereunder read with RBI Directions.

CHAPTER -III

1) RESOLUTION OF DISCREPANCIES:

Each business process shall document and implement procedures to resolve information discrepancies and to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.

2) REPORTING:

The business shall have a system of internal reporting of suspicious transactions, counterfeit transactions and cash transactions greater than Rs.10 lakhs, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.

“Suspicious transaction” means a 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 the proceeds of crime; or
- b) appears to be made in circumstances of unusual or unjustified complexity; or
- c) appears to have no economic rationale or bona fide purpose; or
- d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
- e) Where the transactions are abandoned by customers on being asked to give some details or to provide documents.

Branch Sales Manager/Branch Credit Manager/ Branch In-charge to give the required details of Cash Transactions [Rs.10 lakhs and above or its equivalent in foreign currency in one transaction or series of related transaction in any account(s)] and Suspicious Transaction(s), to the Company Secretary & Compliance Officer of the Company, promptly upon detecting the same and the Company Secretary & Compliance Officer, to report the said Transaction(s) to FIU-India, as per the PMLA Act and the rules made thereunder.

The Company to place the details of Cash Transactions and Suspicious, as above before the Audit Committee/Board of Director, on periodically basis, as per the applicable provisions of Act and the Rules and the Board of Directors to ensure the compliance of the same.

Illustrative list of activities which would be construed as suspicious transactions are given in **Annexure-IV** to this policy.

Further, the Principal officer shall furnish information of the above mentioned transactions to the Director, Financial Intelligence Unit - India (FIU-IND) at the prescribed address in the formats prescribed in this regard including the electronic filing of reports.

Provided that where the Principal officer, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued greater than Rs.10 lakhs so as to defeat the provisions of the PMLA regulations, such officer shall

furnish information in respect of such transactions to the Director within the prescribed time.

The Company shall not put any restriction on operations in the accounts where a suspicious transaction report (STR) has been filed. The Company shall keep the fact of furnishing of STR strictly confidential and shall ensure that there is no tipping off to the customer at any level.

The Company shall upload the KYC information pertaining to individuals / legal entities, as applicable from time to time, with Central KYC Records Registry (CKYCR) within 10 days of commencement of account-based relationship with the customer, in terms of provisions of the RBI Directions read with Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

3) RECORDS RETENTION:

Each business process shall document and implement appropriate procedures to retain records of KYC due diligence and anti-money laundering measures. The business process shall implement, at a minimum, the following procedures for retaining records:

a. Transactions for which records need to be maintained:

- i. All cash transactions of the value of more than Rs.10 lakhs or its equivalent in foreign currency.
- ii. 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.
- iii. 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.
- iv. All suspicious transactions whether or not made in cash.

b. Information to be preserved:

The information required to be preserved with respect to the above transactions are the nature of transactions, amount and the currency in which it was denominated, date of transaction and the parties to the transaction.

c. Periodicity of retention:

The following records shall be retained for a minimum period of five years after the business relationship is ended:

- i. The customer identification information and residence identification information including the documentary evidence thereof.
- ii. All other necessary records pertaining to the transactions that could be produced as evidence for prosecution of persons involved in criminal activity.

Further, a description of the methods used to verify customer identity as well as a description of the resolution of any discrepancies in verification shall be maintained for a period of at least Ten (10) years after such record was created. The above records shall be maintained either in hard or soft format and shall be made available to the competent authorities upon request.

4) EXISTING CUSTOMERS:

The requirements of the earlier sections are not applicable to accounts opened by existing customers, provided that the business process has previously verified the identity of the customer and the business process continues to have a reasonable belief that it knows the true identity of the customer. Further, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the due diligence measures.

5) ENHANCED DUE DILIGENCE:

The Company is primarily engaged in retail finance. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The Company shall conduct **Enhanced Due Diligence** in connection with all customers or accounts that are determined to pose a potential high risk and are determined to warrant enhanced scrutiny. Each business process in its credit policy shall establish appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting appropriate additional due diligence or investigative actions beyond what is required by standard KYC due diligence. Enhanced Due Diligence shall be coordinated and performed by the Company, who may engage appropriate outside investigative services or consult appropriate vendor sold databases when necessary. Each business process shall establish procedures to decline to do business with or discontinue relationships with any customer when the Company cannot adequately complete necessary Enhanced Due Diligence or when the information received is deemed to have a significant adverse impact on reputational risk.

The following are the indicative list where the risk perception of a customer may be considered higher:

- (i) Customers requesting for frequent change of address/contact details
- (ii) Sudden change in the loan account activity of the customers

(iii) Frequent closure and opening of loan accounts by the customers

Enhanced due diligence may be in the nature of keeping the account monitored closely for a re-categorisation of risk, updation of fresh KYC documents, field investigation or visit of the customer, etc., which shall form part of the credit policies of the businesses.

6) RELIANCE ON THIRD PARTY DUE DILIGENCE:

For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, the Company may rely on a third party; subject to the conditions that- the Company obtains records or information of such customer due diligence carried out by the third party within two days from the third party or from Central KYC Records Registry;

- a) the Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
- b) the Company is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;
- c) the third party is not based in a country or jurisdiction assessed as high risk; and
- d) the Company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

CHAPTER -IV

1) RISK CATEGORISATION:

The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization of customers will be carried out from time to time.

The Company shall have a system in place for periodical updation of customer identification data after the account is opened. Full KYC exercise will be done at a periodicity not less than once in ten years in case of low risk category customers, not less than once in eight years in case of medium risk category customers and not less than once in two years in case of high risk category customers.

Low risk category customers need not submit fresh proofs of identity and address at the time of periodic updation, in case of no change in status with respect to their

identities and addresses and a self-certification by the customer to that effect shall suffice in such cases. In case of change of address of such 'low risk' customers, they can forward a certified copy of proof of address by mail/post, etc.

In case any existing customer fails to submit PAN or equivalent e-document or Form No.60, the Company may temporarily cease operations in the account till the time the same is submitted by the customer. For the purpose of ceasing the operation in the account, only credits shall be allowed.

However, for customer who are unable to provide PAN or equivalent e-document or Form No.60 owing to injury, illness or infirmity on account of old age or such like causes, the Company will continue operation of accounts for such customers subject to enhanced monitoring of the accounts.

All the customers under different product categories are categorized into low, medium and high risk based on their profile. The Credit manager while appraising the transaction and rendering his approval will prepare the profile of the customer based on risk categorization. An indicative categorization for the guidance of businesses is provided in Annexure - I. Each business process adopts the risk categorization in their respective credit policies subject to confirmation by compliance based on the credit appraisal, customer's background, nature and location of business activity, country of origin, sources of funds, client profile, etc., Where businesses believe that a particular customer falling under a category mentioned below is in his judgement falling in a different category, he may categorise the customer so, so long as appropriate justification is provided in the customer file.

2) MONITORING OF TRANSACTIONS:

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The different business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible legitimate purpose. High-risk accounts have to be subjected to intensified monitoring.

3) RISK MANAGEMENT:

The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

Company's internal audit function play a role in evaluating and ensuring adherence to the KYC policies and procedures. Internal Auditors specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

The compliance in this regard is put up before the Audit Committee / Board from time to time.

The Company ensures that the decision-making functions of determining compliance with KYC norms are not outsourced.

4) Hiring of Employees and Employee training:

- a. Adequate screening mechanism as an integral part of personnel recruitment/ hiring process to be in place.
- b. On-going employee training programme be in place so that the members of staff are adequately trained in KYC & AML Measures policy. The focus of the training be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff will be specially trained to handle issues arising from lack of customer education.
- c. BHFL shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. BHFL must also seek to create an environment that encourages open communication and high integrity among its employees.
- d. Proper staffing of the audit function with persons adequately trained and well-versed in KYC / AML / CFT policies of the company, regulations and related issues should be ensured.

Know Your Employee (KYE) / Staff Policy

(As part of the KYC Policy of the NBFC)

In accordance with the RBI Master Direction – Know Your Customer (KYC) Direction, 2016, as amended from time to time, and considering the risk-based approach expected of Regulated Entities (REs), the Company adopts the following Know Your Employee (KYE) / Staff Policy as an integral part of its governance and compliance framework.

a. Objective

To ensure that individuals employed by the Company, particularly in sensitive or compliance-related functions, are of verified integrity and competence, and that no employee poses a reputational, regulatory, or operational risk to the NBFC.

b. Applicability

This policy applies to all categories of employees – permanent, temporary, contractual, interns, and outsourced staff – engaged by the Company at any location, including those in roles involving:

- Customer onboarding and servicing,
- KYC/AML/CFT compliance,
- Loan appraisal and disbursement,
- IT system access,
- Finance, legal, and internal audit functions.

c. Pre-employment Screening

A risk-based screening process shall be conducted before appointment, which shall include the following (as applicable to the role):

- **Identity verification** through Aadhaar, PAN, and other valid government-issued documents.
- **Educational and professional qualification verification.**
- **Employment history and reference checks**, including reasons for leaving previous roles.
- **Criminal background verification**, through police verification or third-party agency checks, especially for staff in sensitive functions.
- **Credit bureau report check** for employees involved in credit, treasury, or finance functions.
- **Fit and proper declaration**, as applicable for key managerial positions.

The outcome of the screening shall be recorded and retained securely in the employee file.

d. Post-Employment Vigilance and Monitoring

- Employee behaviour and adherence to the Code of Conduct shall be monitored on an ongoing basis.
- Any adverse information post-joining, including regulatory violations or unethical conduct, shall be reviewed and dealt with under the Disciplinary Policy.
- The Company may re-verify credentials or seek updated declarations at its discretion.

e. Training and Awareness

The Company shall ensure that staff involved in KYC/ AML/ CFT or frontline operations receive regular training, covering:

- KYC documentation and onboarding processes,
- Detection and reporting of suspicious transactions,
- Regulatory developments and red flag indicators,
- Data protection and customer privacy norms.

Such training shall be held at least annually and documented as part of the compliance program.

f. Fostering a Culture of Integrity

- The Company shall promote a work environment that encourages ethical behaviour, transparency, and open communication.
- Employees shall be encouraged to report any suspicious internal activity or misconduct via a defined whistleblower mechanism.

g. Record Keeping and Confidentiality

- All documents collected under the KYE process shall be securely maintained and made available to regulators, if required.
- Employee personal information shall be handled with strict confidentiality and used only for internal risk management purposes.

5) APPOINTMENT OF DESIGNATED DIRECTOR / PRINCIPAL OFFICER:

Board has appointed the Designated Director and Principal Officer as required under PMLA Act and the Rules.

In case of any discrepancy or amendment/change in the RBI Directions with respect to KYC & AML, the said Directions shall automatically applied to the Company.

6) Non-Account-Based Relationships

Scope Clarification:

The Company does not maintain any account-based relationship as it offers only project loans. Accordingly, KYC procedures shall be applied in accordance with the RBI Master Direction – Know Your Customer (KYC), 2023, specifically for one-time transactions, including disbursement of project loans, in accordance with applicable norms for walk-in or non-account holders engaging in financial transactions of Rs. 50,000 or more.

7) Unique Customer Identification Code (UCIC)

UCIC Allocation:

The Company shall allot a Unique Customer Identification Code (UCIC) to each borrower for tracking customer relationships and transactions in compliance with RBI guidelines.

8) CDD for One-Time High-Value Transactions

One-Time Transaction Threshold:

Where the Company undertakes financial transactions equal to or exceeding Rs. 50,000 with a borrower or entity without establishing an account, Customer Due Diligence (CDD) shall be carried out as per the requirements of the Master Direction.

9) Ongoing Due Diligence in Project Lending

Project Loan Monitoring:

The Company shall conduct ongoing due diligence during the life cycle of each project loan to ensure that disbursements and end-use of funds are in line with the stated purpose and customer profile. Any inconsistencies shall trigger a review of the risk categorisation and may warrant enhanced scrutiny.

10) Beneficial Ownership in Legal Entities

Identification of Beneficial Owners:

The Company shall identify and verify the beneficial owners of borrowing entities as per Rule 9(3) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, except in cases where the entity is a listed company or a wholly-owned subsidiary of a listed company, in which case exemption shall apply as per RBI norms.

11) Risk Assessment of New Products or Delivery Channels

Product Risk Assessment:

Before launching any new financial product or delivery mechanism, the Company shall conduct a documented risk assessment to evaluate potential Money Laundering/Terrorist Financing (ML/TF) vulnerabilities and apply appropriate due diligence and monitoring measures.

Annexure – I

Indicative list for Risk Categorization

Parameters	Low Risk (1)	Medium Risk (2)	High Risk (3)
Land Ownership & Due Diligence	Authorities/Company	Joint venture	Private-owned/Individual
RERA Due Diligence	Registered, all approvals	Registered, minor gaps	Not registered, major issues
Land Documents & Agreements	Clear & verified	Minor discrepancies	Title disputes/missing
CIBIL Score	750+	650-750	Below 650
Asset Coverage	3x collateral value	2x collateral value	1x collateral value
Entity Type	Govt entity/Co-op Society	Pvt/Public Co., LLP, Trusts	Individual/Unregistered
Past Projects	Completed projects	Limited experience	No completed projects
Existing Liabilities	No past liabilities	Manageable liabilities	High liabilities
Guarantee Type	Corporate guarantee	No guarantee	Personal guarantee
Promoter Contribution	High contribution	Moderate contribution	Low contribution
Location-Wise Sales Rate	High demand/increasing	Moderate demand/fluctuating	Low demand/declining

1. Points:

- Low Risk: 1 point
- Medium Risk: 2 points
- High Risk: 3 Points

2. Overall Risk Calculation:

- Total Score 11-18 → Low Risk
- Total Score 19-25 → Medium Risk
- Total Score 26-33 → High Risk

Annexure - II

Customer Identification Requirements

Trust/Nominee or Fiduciary Accounts

In the case of any application from trust/nominee or fiduciary accounts, the Company determines whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary.

If in doubt of the persons behind the customer, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. Company takes reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Accounts of companies and firms

Company needs to be vigilant against business entities being used by individuals as a 'front' for transactions. Company should examine the control structure of the entity and identify the natural persons who have a controlling interest and who comprise the management.

These requirements may be moderated according to the risk perception e.g. in the case of a public company.

Client accounts opened by professional intermediaries

Where the transaction is with a professional intermediary who in turn is on behalf of a single client, that client must be identified. The Company shall not open accounts with such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Company.

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.

The Company offers products primarily to Indian residents only. The Company if extending any finance to non-residents should check if he is PEP and check all the

information available about the person in the public domain. The decision to transact with the PEP should be taken only by the Head of credit of the respective businesses supported by appropriate verification. The Company is also required to subject such accounts to enhanced monitoring on an ongoing basis. The above norms shall also be applied to the contracts of the family members or close relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the approval of the Head of respective businesses shall be obtained to continue the business relationship and subject the account to the KYC due diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

Accounts of non-face-to-face customers

The Company will not do any transactions with non-face-to-face customers.

Identity of Beneficial Owner

The Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a customer and/or the person on whose behalf the transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership

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

Explanation:

- I. "Controlling ownership interest" means ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company;
- II. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

(b) where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than fifteen percent of capital or profits of the partnership;

(c) where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

(d) 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;

(e) 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 fifteen percent 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. In case the customer is acting on behalf of another person as trustee / nominee, the Company shall obtain satisfactory evidence of the identity of the persons on whose behalf they are acting; and

where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

Annex-III

Customer Identification Procedure – KYC documents that may be obtained from customers (Officially Valid Documents)

Nature of customer	List of applicable documents
Individual	The Company shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity; a) proof of possession of Aadhaar number where offline verification can be carried out; or b) a certified copy of any OVD containing details of his identity and address; and c) the Permanent Account Number (PAN) or Form no.60; and d) such other documents as specified by the Company from time to time. List of OVDs: i) Passport (Valid) ii) Driving license iii) Proof of possession of Aadhaar number/ Aadhaar (Optional) iv) Voter's identity card issued by the Election Commission of India v) Job card issued by NREGA duly signed by an officer of the State Govt. vi) 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 UIDAI. b. where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:- 1) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); 2) property or Municipal tax receipt;

	3) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
	4) letter of allotment of accommodation from employer issued by State Govt. or Central Govt. 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 '(2)' above e. 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: 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.

Sole Proprietary firms	I. Customer due diligence of the individual proprietor shall be carried out as applicable / specified for Individual. II. In addition to the above, any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained: a) Registration certificate b) Certificate/licence issued by the municipal authorities under Shop and 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 DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. 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, landline telephone bills, etc. Explanation: In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at its discretion, accept only one of those documents as proof of business/activity after recording the appropriate reason for accepting one document. The Company shall undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.
------------------------	---

	business/activity after recording the appropriate reason for accepting one document. The Company shall undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.
Company	Certified copies of each of the following documents shall be obtained: - Certificate of incorporation - Memorandum and Articles of Association - Permanent Account Number of the company - A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf - Documents, as specified for Individual, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
Partnership Firm	Certified copies of each of the following documents shall be obtained: - Registration certificate - Partnership deed - Permanent Account Number of the partnership firm - Documents, as specified for Individual, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
Trust	Certified copies of each of the following documents shall be obtained: - Registration certificate - Trust deed - Permanent Account Number or Form No.60 of the trust - Documents, as specified for Individual, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
Unincorporated Association or a Body of Individuals	Certified copies of each of the following documents shall be obtained: - Resolution of the managing body of such association or body of individuals - Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals - Power of attorney granted to transact on its behalf - Documents, as specified for Individual, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and - Such information as may be required by the Company to collectively

	establish the legal existence of such an association or body of individuals. Explanation: I. Unregistered trusts / partnership firms shall be included under the term 'unincorporated association'. II. Term 'body of individuals' includes societies.
Juridical persons not specifically covered above, such as societies, universities and local bodies like village panchayats	Certified copies of the following documents shall be obtained: i) Document showing name of the person authorised to act on behalf of the entity; ii) Documents, as specified for Individual, of the person holding an attorney to transact on its behalf and iii) Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

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

Annexure - IV

Illustrative list of activities which would be construed as suspicious transactions

Activities which are not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits shall be construed as suspicious transactions.

Any attempt to avoid reporting / record-keeping requirements / provides insufficient / suspicious information:

- a. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
- b. Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
- c. An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.
- d. Certain Employees of the Company arousing suspicion:
- e. An employee whose lavish lifestyle cannot be supported by his or her salary.
- f. Negligence of employees / willful blindness is reported repeatedly.
- g. Some examples of suspicious activities/transactions to be monitored by the operating staff:
- h. Multiple accounts under the same name
- i. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds are doubtful etc;
- j. There are reasonable doubts over the real beneficiary of the loan.
- k. Frequent requests for change of address.
