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

Policy Name	Policy on Know Your Customer (KYC) and Anti-Money Laundering (AML) Measures
Company Name	Jayshree Credit Services Private Limited
Approved By	Board of Directors
Effective Date	1st April 2026
Version	V3
Review Frequency	Annual / As required by applicable law

CHAPTER I

INTRODUCTION

The Reserve Bank of India ("RBI") has issued Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 including comprehensive guidelines on Know Your Customer (KYC) norms and Anti- Money Laundering (AML) / Countering the Financing of Terrorism ("CFT") standards and has advised all Regulated Entities, including NBFCs to ensure that a proper policy / framework on KYC and AML/CFT measures be formulated and put in place with the approval of the Board.

The Policy shall be based on a risk-based approach and shall incorporate Customer Acceptance Policy, Risk Management, Customer Identification Procedure (CIP) and Monitoring of Transactions and shall also include provisions relating to periodic updation of KYC, record management, and reporting obligations to FIU-IND in accordance with applicable law.

Accordingly, in compliance with the guidelines issued by the RBI, the following KYC and 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 Jayshree Credit Services Private Limited ("Company"). This Policy shall also apply to business verticals, delivery channels, outsourced service providers to the extent applicable, and employees / officials responsible for onboarding, monitoring, and reporting obligations under the applicable law.

Any changes to the Policy shall be made with the approval of the Board of Directors or any committee to which the Board has delegated such power.

The Company shall ensure compliance with the Prevention of Money-Laundering Act, 2002, the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, the RBI KYC Directions, 2025, the Unlawful Activities (Prevention) Act, 1967, and other applicable laws, rules, circulars, and regulatory instructions.

The Company shall carry out periodic Money Laundering / Terrorist Financing ("ML/TF") risk assessment exercises to identify, assess and take effective measures to mitigate risks relating to clients, countries or geographic areas, products, services, transactions, and delivery channels. Such assessment shall be properly documented, reviewed at least annually, and placed before the Board or the relevant committee of the Board and appropriate risk mitigation measures shall be implemented based on such assessment.

DEFINITIONS

"Act" and "Rules" mean the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively as amended from time to time.

"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.

"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.

"CKYC Identifier" means a 14- digit KYC Identifier Number (KIN) which is issued upon successful submission/ registration of KYC Documents of the Borrower on CERSAI Portal. An SMS or email will be sent to the Borrower, once the KIN is generated. The Company shall ensure that the KYC Identifier is communicated to the Customer in accordance with RBI requirements. In case the Company generates the KIN for any customer, under due requisite authorization, the Company shall ensure that the KIN is communicated to the Customer (either individual/Legal Entity).

"Beneficial Owner" means 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 entity. The procedure for determination of Beneficial Ownership shall be as follows:

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:

"Controlling ownership interest" means ownership of or entitlement to more than ten percent of shares or capital or profits of the company;

"Control" shall include the right to appoint the majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

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 ten percent of capital or profits of the partnership; or who exercises control through other means;

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;

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;

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 ten 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.

"Certified Copy" 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.

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

a) A person or entity that maintains an account and/or has a business relationship with the Company including;
b) customers associated with the selling/marketing of permitted insurance business, if any, of the Company;
c) One on whose behalf the account is maintained (i.e. the beneficial owner);
d) Beneficiaries of transactions conducted by professional intermediaries such as Stockbrokers, Company Secretaries, Chartered Accountants, Solicitors etc. as permitted under the law, and;
e) 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;

"Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification and obtaining information on the purpose and intended nature of the business relationship.

"Customer identification" means undertaking the process of CDD.

"Designated Director" means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

the Managing Director or a whole-time Director, duly authorised by the Board of Directors, where the Company is a company. The Company shall communicate the name, designation, address and contact details of the Designated Director to FIU-IND and RBI. The Principal Officer shall not be nominated as the Designated Director.

"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).

"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.

"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 Taxpayers hold a substantial ownership interest.

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

"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.

"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.

"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 and risk categorisation.

"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 based on risk categorization of customers.

"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.

"Principal Officer" means an officer nominated by the Company responsible for furnishing information under Rule 8 of the PML Rules. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under applicable law. The Company shall communicate the name, designation, address, and contact details of the Principal Officer to FIU-IND and RBI.

"Regulated Entity (RE)" includes NBFCs governed by RBI Directions.

"Suspicious Transaction" means a transaction, 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 have no economic rationale or bona fide purpose; or (d) gives rise to a reasonable ground of suspicion that it may involve financing of activities relating to terrorism.

CHAPTER II

CUSTOMER ACCEPTANCE POLICY:

The Company shall follow the listed norms while onboarding a customer for a loan:

No loan account shall be opened in anonymous or fictitious or benami name.

The Company shall carry out customer due diligence (CDD) before onboarding. When the identity of the applicant is not known or the Company is unable to apply appropriate CDD measures, no transaction or account-based relationship will be undertaken with such person / entity. The Company shall file an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer in accordance with FIU-IND reporting requirements.

Optional/additional information shall be obtained with the explicit consent of the customer after the loan account is opened. Where additional information is not specified in the internal KYC policy as mandatory, the same shall be obtained only with the explicit consent of the customer and the Company shall clearly distinguish between mandatory and optional KYC information.

The Company shall apply CDD measures at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of the Company desires to open another account with the Company, there shall be no need for a fresh CDD exercise for identification purposes, subject to risk based review.

Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority. Where equivalent e-documents are obtained, the customer's digital signature shall also be verified in accordance with the Information Technology Act, 2000. Where GST details are available, the GST number shall be verified from the search / verification facility of the issuing authority.

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

The illustrative list of such risk categorisation is provided in Annexure – I.

The Company shall documents the rationale for risk categorization and maintain confidentiality of such categorization to avoid tipping off.

The customer profile contains mandatory information to be sought for KYC purpose relating to customer's identity, address, nature of business activity, information about the clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile the Company will seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein

will not be divulged for cross-selling or any unrelated purpose. The Company shall maintain secrecy regarding customer information except where the disclosure is mandated by law/regulation/authority and/or there is a duty to the public to disclose and/or the disclosure is made with express or implied consent of the customer.

The Company shall ensure that the identity of the customer does not match any person or entity whose name appears in the sanction lists circulated/prescribed by RBI from time to time. Such screening shall also include lists required under applicable UAPA / UNSC-related directions and FATF public statements, where applicable..

The intent of the Policy is not to result in denial of financial services to public, especially to those, who are financially or socially disadvantaged. While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers. The Company shall not reject an application for onboarding or periodic updation of KYC without application of mind, and the concerned officer shall record the reasons for rejection.

When the true identity of the account holder is not known, the Company shall file Suspicious Transaction Reporting (STR). Where the Company forms a suspicion of money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip off the customer, it shall not pursue the CDD process and shall instead file an STR with FIU-IND without delay and in accordance with applicable timelines.

The Company shall also clearly spell out the circumstances in which a customer is permitted to act on behalf of another person / entity and shall follow the CDD procedure for all joint account holders, wherever applicable.

The Company shall:

a. not undertake any transaction or establish any account-based relationship without completing CDD procedures;
b. specify the mandatory information required for KYC at the time of onboarding and periodic updation;
c. ensure that decision-making functions relating to KYC compliance are not outsourced;
d. implement appropriate systems to detect and prevent money laundering and terrorist financing risks.

CUSTOMER IDENTIFICATION PROCEDURE:

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 before commencement of the loan account relationship in accordance with RBI KYC Directions, 2025. Customer identification means identifying the customer and verifying their identity by using reliable and independent sources of documents, data or information to ensure that the customer is not a fictitious/ anonymous or benami person.

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 to include 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). Accordingly, the business processes of the Company are required to:

(1) verify the identity of any Person or the entity transacting with the Company.
(2) maintain records of the information used to verify a customer's identity, including name, address and other identifying information.
(3) 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 by and periodically circulated by the United Nations Security Council (UNSC) and whose names appears in the sanction's lists circulated by Reserve Bank of India. The Company may use the website of the concerned authority and/or a compliant third-party screening service provider for such verification, subject to applicable law.

Details of accounts/ customers bearing resemblance to 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 without delay.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on certain customers by putting in place reasonable measures 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 in line with the Risk- Based Approach prescribed by RBI.

The Company shall undertake identification of customers prior to commencement of a loan account-based relationship with the customer and when there is a doubt about the authenticity or adequacy of the customer identification data it has obtained. The Company shall also undertake identification in the case of walk-in / non-account-based transactions equal to or exceeding ₹50,000, whether as a single transaction or several connected transactions, and where the Company has reason to believe that a customer is intentionally structuring transactions below the threshold to avoid reporting requirements.

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 and such procedures shall be documented and subject to periodic review.

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, such as:

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 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: For an individual, a residential or business street address. For a person other than an individual (such as a corporation, partnership, or trust), the registered office/principal place of business, local office, or other physical location in accordance with Officially Valid Documents (OVD) requirements.
d) Telephone/Fax number/E-mail ID where applicable
e) Identification number: PAN, Passport Number and Country of Issuance, Proof of Possession of Aadhaar 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 blacks-out their Aadhaar number before submitting the same to the Company, unless the Aadhaar number in full is provided voluntarily by the customer.
f) One recent photograph of the individual customer - 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 provided as Annexure- III to this policy.

CUSTOMER DUE DILIGENCE (CDD)/VERIFICATION:

Verification of customer identity shall 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 in accordance with the Risk- Based Approach prescribed by RBI.

VERIFICATION THROUGH OFFICIALLY VALID DOCUMENTS IN CASE OF INDIVIDUALS:

Comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or Officially Valid Document so submitted 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 those specified 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.

VERIFICATION THROUGH DOCUMENTARY OR NON-DOCUMENTARY METHODS IN CASE OF ENTITIES:

These methods may include, but are not limited to the following:

(a) Contacting or visiting a customer.
(b) Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer's reporting agency, public database, or other source.
(c) Unique Code Verification, wherein a Unique Code is sent to the entity's address through physical dispatch services, and the customer is required to confirm the code over email, which verifies the declared registered/corporate address of the entity.
V-KYB process, wherein Customer conducts a self-recording video capturing the establishment with photos as per required parameters and the mobile application or the link also captures the location in a verifiable manner with the given corporate address by the customer.
(d) Verification of beneficial ownership and control structure of the entity.

VERIFICATION BASED ON DIGITAL KYC:

The Company may undertake the Digital KYC process for CDD in which live photograph of the customer will be captured and officially valid document or the proof of possession of Aadhaar shall 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 Company, as per the provisions contained in the Prevention of Money Laundering Act, 2002 and the rules made thereunder read with RBI Directions. The detailed procedure for Digital KYC shall be formulated in accordance with this Policy, as a Standard Operating Procedure ("SOP") by the compliance team with due approval from the Designated Director shall be kept on record in a retrievable format for periodical checks as may be required.

VIDEO CUSTOMER IDENTIFICATION PROCESS (V-CIP):

A method of customer identification by an official of the Company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face.

The Company may undertake live V-CIP for establishment of a loan account relationship with an individual customer after obtaining their informed consent and adhering to the procedures prescribed in RBI regulations. This process shall be treated as face-to-face process for the purpose of customer identification.

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.

The entire data and recordings of V-CIP shall be stored in a system located in India. The Company 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 the RBI Master Direction on KYC, shall also be applicable for V-CIP including retention for the prescribed period.

The activity along with the credentials of the official performing the V-CIP shall be preserved. The detailed

procedure of V-CIP formulated in accordance with this Policy, as a Standard Operating Procedure ("SOP") by the compliance team with due approval from the Designated Director and shall be kept on record in a retrievable format for periodical checks as may be required.

Reliance on third-party CDD may be undertaken only subject to applicable RBI conditions, including immediate availability of CDD records, regulatory supervision of the third party, and continued ultimate responsibility of the Company for customer due diligence and record keeping compliance.

The Company shall apply Enhanced Due Diligence (EDD) in the following cases:

a. High-risk customers
b. Politically Exposed Persons (PEPs)
c. Non-face-to-face customers
d. Customers from high-risk jurisdictions

EDD measures shall include:

a. Obtaining senior management approval
b. Verifying source of funds and source of wealth
c. Conducting enhanced monitoring of transactions

CHAPTER III

RESOLUTION OF DISCREPANCIES:

Each business process shall 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.

REPORTING:

"Suspicious Transaction" means a transaction whether made in cash or not 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) attempted or abandoned transactions, including where customers abandon the transaction on being asked to provide details or documents, may also be examined and reported where required under applicable law/internal process.

The Company shall place the details of Suspicious Transactions before the Audit Committee/Board of Directors, on periodical basis, as per the applicable provisions of the Act and the Rules and the Designated Director shall 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/Designated Director 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. The Principal Officer shall be primarily responsible for

furnishing such information under the law.

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 30 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.

The Company shall maintain records and furnish reports to FIU-IND in accordance with the PMLA, the PML Rules, and the applicable RBI Directions, including but not limited to suspicious transaction reporting and any other reporting obligations applicable to the Company from time to time.

RETENTION OF RECORDS:

The Company shall 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:

PERIODICITY OF RETENTION

The following records shall be retained by the Company in the manner as specified below:

(a) The customer identification information and residence identification information including the documentary evidence thereof of every customer shall be retained by the Company for a minimum period of five years after the business relationship is ended; and
(b) All other necessary records pertaining to the transactions between the Company and the customers shall be retained by the Company for a minimum period of five years from the date of such transaction.

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 five years after such record was created.

All records as mentioned above shall be maintained either in hard or soft format and shall be made available to the competent authorities upon request.

ENHANCED DUE DILIGENCE:

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. The Company 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 sourced databases when necessary. The Company 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 for the Company.

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

a) Customers requesting for frequent change of address/contact details
b) Sudden change in the loan account activity of the customers
c) Frequent closure and opening of loan accounts by the same customers
d) Non-face-to-face customers
e) Politically Exposed Persons and their family members / close relatives, as applicable
f) Customers from high-risk jurisdictions or where adverse sanctions / ML/TF indicators are noted

Enhanced due diligence may be undertaken by various methods such as keeping the account monitored closely for recategorization of risk, updating fresh KYC documents, field investigation or physical meeting/visit with the customer.

RELIANCE ON THIRD PARTY DUE DILIGENCE:

The Company may rely on customer due diligence carried out by a third party, subject to the conditions prescribed under applicable RBI Directions, including obtaining CDD records / information immediately from the third party or CKYCR, ensuring that the third party is regulated / supervised and compliant with CDD and record-keeping requirements, ensuring that the third party is not based in a high-risk jurisdiction where prohibited, and recognising that the ultimate responsibility for customer due diligence and related obligations shall remain with the Company.

CHAPTER IV

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 should 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 customers who are unable to provide PAN or equivalent e-documents 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 teams, while appraising the transaction and rendering their approval, will prepare the profile of the customer based on risk categorization. An indicative categorization 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 credit teams believe that a particular customer falling under a category mentioned above is, in their judgement, falling in a different category, the customer may be so categorized, after appropriate justification is provided in the customer file by the credit team.

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 plays a role in evaluating and ensuring adherence to the KYC policies and procedures. Internal Auditors specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard.

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

Quarterly audit notes and compliance shall be submitted to the Audit Committee, in line with the applicable RBI Directions.

The Company shall specify who constitutes "Senior Management" for the purpose of KYC compliance, allocate responsibility for effective implementation of this Policy, and ensure independent evaluation of compliance functions. The Company shall not outsource the decision-making functions of determining compliance with KYC norms.

ANNEXURE - II

CUSTOMER IDENTIFICATION REQUIREMENTS

Trust/Nominee or Fiduciary Accounts
The Company shall clearly identify whether the customer is acting on behalf of another person and obtain satisfactory evidence of the identity of intermediaries and the people on whose behalf they are acting, along with details of the nature of the trust / fiduciary arrangement.

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.

In the event the Company feels that the customer is a face for people acting behind it, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the people 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 settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Accounts of Companies and Firms

The Company shall remain vigilant against business entities being used by individuals as a front for transactions and shall examine the ownership and control structure of the entity to identify the natural persons having controlling interest and those comprising management.

These requirements may be moderated according to 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 acting 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 client details to the Company.

The Company shall not open accounts with professional intermediaries who are bound by client confidentiality provisions that prohibit disclosure of client details where such disclosure is required for compliance with applicable KYC / AML obligations.

Accounts of Politically Exposed Persons (PEPs) Resident Outside India

Politically exposed people 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 the customer is a 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 Designated Director supported by appropriate verification. The Company is also required to subject such accounts to enhance monitoring on an ongoing basis. The above norms shall also be applied to the accounts / customers of the family members or close relatives of PEPs. The decision to establish or continue a relationship with a PEP shall be taken at an appropriately senior level / by the Designated Director in accordance with internal policy, and such relationship shall be subject to enhanced ongoing monitoring.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the approval of the Designated Director 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.

ANNEXURE-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 power of attorney holder related to any legal entity: (i) proof of possession of Aadhaar number where offline verification can be carried out; or where offline verification cannot be carried out, a certified copy of proof of possession of Aadhaar number; or a certified copy of any OVD containing details of identity and address; and (ii) PAN or Form No. 60; and (iii) such other documents as specified by the Company from time to time. 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 power of attorney holder related to any legal entity: (i) proof of possession of Aadhaar number where offline verification can be carried out; or where offline verification cannot be carried out, a certified copy of proof of possession of Aadhaar number; or a certified copy of any OVD containing details of identity and address; and (ii) PAN or Form No. 60; and (iii) such other documents as specified by the Company from time to time. **List of OVDs:** Passport; Driving Licence; Proof of possession of Aadhaar number; 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. **Provided that:** where the customer submits proof of possession of Aadhaar number as an OVD, he/she may submit it in such form as issued by UIDAI; where the OVD furnished does not contain updated address, the following may be deemed OVDs for the limited purpose of proof of address: utility bill not more than two months old, property or municipal tax receipt, pension or family pension payment orders, letter of allotment of accommodation from employer issued by Government / statutory / regulatory bodies / PSU / scheduled commercial banks / financial institutions / listed companies, and leave and licence agreements with such employers allotting official accommodation; provided the customer submits OVD with current address within three months; where the OVD presented by a foreign national does not contain address details, documents issued by Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India may be accepted as proof of address.
Sole Proprietary Firms	In addition to the documents applicable to an individual proprietor, the Company shall obtain any two of the following documents as proof of business / activity in the name of the proprietary firm: (i) registration certificate; (ii) certificate / licence issued by the municipal authorities under the Shop and Establishment Act; (iii) sales and income tax returns; (iv) CST / GST certificate; (v) certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities; (vi) IEC (Importer Exporter Code) issued by DGFT; (vii) licence / certificate of practice issued in the name of the proprietary concern by any

	professional body incorporated under a statute; (viii) complete Income Tax Return (not just acknowledgement) in the name of the sole proprietor showing the firm's income and duly authenticated / acknowledged by the Income Tax authorities; (ix) utility bills in the name of the proprietary concern; or (x) such other documents as may be accepted under applicable RBI Directions. Where it is not possible to furnish two such documents, the Company may, at its discretion, accept one such document with reasons recorded, undertake contact point verification, and obtain such other information / clarification as may be necessary to establish the existence of the firm.
Company	Certified copies of each of the following documents shall be obtained: (i) Certificate of Incorporation; (ii) Memorandum and Articles of Association; (iii) Permanent Account Number of the company; (iv) Resolution of the Board of Directors and power of attorney granted to its managers, officers, or employees to transact on its behalf; and (v) documents, as specified for an Individual, relating to the beneficial owner, 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: (i) registration certificate, if registered; (ii) partnership deed; (iii) Permanent Account Number of the partnership firm or Form No. 60; and (iv) documents, as specified for an Individual, relating to the beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on the firm's behalf.
Trust	Certified copies of each of the following documents shall be obtained: (i) registration certificate, if registered; (ii) trust deed; (iii) Permanent Account Number or Form No. 60 of the trust; and (iv) documents, as specified for an Individual, relating to the 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: (i) resolution of the managing body of such association or body of individuals; (ii) Permanent Account Number or Form No. 60 of the unincorporated association or body of individuals; (iii) power of attorney granted to transact on its behalf; and (iv) documents, as specified for an Individual, relating to the beneficial owner, persons holding an attorney to transact on its behalf, and such other authorised signatories / managers as may be applicable.