



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

DHANRISE FINANCE PRIVATE LIMITED

Non-Banking Financial Company – Base Layer (Non-Deposit Taking)

CIN: U64990UW2026PTC249231 | RBI Registration No.: 0037/2026
Registered Office: 4th Floor, Plot No. A-23, Sector-9, Gautam Buddha Nagar, Noida,
Uttar Pradesh, India, 201301

Document Control

Title	Know Your Customer (KYC) & Anti-Money Laundering (AML) Policy
Company	Dhanrise Finance Private Limited
Regulatory classification	NBFC – Base Layer (NBFC-BL), non-deposit taking
Policy owner	Compliance Department
Version number	V1.0
Effective date	06-October-2026
Approved by	Board of Directors at its meeting held on 06-October-2026
Review frequency	Annually, or earlier upon any regulatory change

Version	Date	Description of change	Approved by
V1.0	06-October-2026	Policy adopted by Dhanrise Finance Private Limited	Board of Directors

1. BACKGROUND AND OBJECTIVE

Dhanrise Finance Private Limited ("DFPL" or "the Company") is a non-deposit-taking NBFC registered with the Reserve Bank of India ("RBI") and classified in the Base Layer. The Company finances used tractors, used commercial vehicles and used construction vehicles for farmers, transporters, contractors, small businesses and other customers in rural, semi-urban and urban India.

This Policy is framed under the RBI KYC Directions as amended from time to time ("KYC Directions"), the Prevention of Money Laundering Act, 2002 ("PMLA"), the PML (Maintenance of Records) Rules, 2005 ("PML Rules"), the Unlawful Activities (Prevention) Act, 1967 ("UAPA") and the Weapons of Mass Destruction Act, 2005 ("WMD Act"). Its objective is to prevent the Company from being used for money laundering, terrorist financing or fraud; to know its customers and their beneficial owners; and to detect and report suspicious activity – without denying finance to genuine farmers and rural customers who have limited documentation.

The Policy applies to all products, branches, channels and employees, and to dealers, Direct Selling Agents (DSAs) and service providers to the extent they perform any KYC activity for the Company. Where the law requires a stricter control, the stricter requirement shall apply.

2. GOVERNANCE

- **Board:** approves this Policy, ensures adequate resources and reviews the KYC/AML framework at least annually. The Risk Management Committee oversees ML/TF risk and reports to the Board.
- **Designated Director:** a Director designated by the Board, responsible for overall compliance with the PMLA and PML Rules.
- **Principal Officer:** a senior official responsible for KYC/AML implementation, monitoring, reporting to FIU-IND and regulatory liaison.
- The Designated Director and the Principal Officer shall be two different persons. Their names, designations and contact details shall be communicated to FIU-IND and RBI, and any change intimated promptly. (Insert names before publishing.)
- **Senior Management:** for the purpose of KYC compliance, Senior Management shall mean the Managing Director / Whole-time Director, the Chief Executive Officer, the Chief Risk Officer, the Chief Compliance Officer and the Principal Officer, or such other officials as the Board may specify. Responsibility for implementation of this Policy shall be allocated to them as set out in this Policy and the related SOPs.
- Decision-making on KYC compliance shall not be outsourced (see Section 5.6 for outsourcing of KYC-related activities).

3. CUSTOMER ACCEPTANCE POLICY

- No loan shall be given in an anonymous, fictitious or benami name.
- No relationship shall be established where CDD cannot be completed due to non-cooperation or unreliable documents; filing of a Suspicious Transaction Report (STR) shall be considered.
- CDD shall cover all applicants, co-applicants, guarantors, beneficial owners and authorised signatories.
- CDD shall be applied at the Unique Customer Identification Code (UCIC) level. A UCIC shall be allotted to every individual customer, and an existing KYC-compliant customer availing another loan or product shall not be required to undergo fresh identification. No introduction shall be sought for onboarding a customer.

- A person may act on behalf of a customer only as an authorised signatory, or under a valid power of attorney, board / managing body resolution or other legal authority, and CDD of such person shall be carried out.
- PAN (where obtained) shall be verified from the verification facility of the issuing authority, the GST number (where available) from the GST search / verification facility, and the digital signature on any equivalent e-document as per the Information Technology Act, 2000.
- Every customer shall be screened against sanctions lists before onboarding (Section 9).
- Only information required for KYC is mandatory; any additional information shall be collected with consent and not used for cross-selling without consent.
- Procedures shall not deny finance to genuine customers, including farmers, small transport operators, disadvantaged persons and persons with disabilities. Reasons for any rejection shall be recorded.

4. CUSTOMER RISK CATEGORISATION

Customers shall be classified as Low, Medium or High risk based on identity, legal form, occupation, ownership, geography, delivery channel, source of funds and any adverse or sanctions indicators. Customers not clearly Low or High shall be treated as Medium. The rationale shall be recorded and kept confidential. Risk category shall be reviewed periodically and on any trigger event.

Risk factor	Lower risk	Higher risk
Customer / occupation	Farmer with land records; salaried person; transporter or contractor with verifiable contracts	Cash-intensive or hard-to-verify activity; complex or opaque ownership
Channel / geography	Face-to-face or V-CIP; local customer	Non-face-to-face without equivalent assurance; unverified broker; high-risk jurisdiction
Behaviour / screening	Repayment consistent with income; no adverse match	Unexplained cash or lump-sum repayment; PEP; adverse media or sanctions proximity

5. CUSTOMER IDENTIFICATION AND DUE DILIGENCE (CDD)

CDD shall be completed before sanction or disbursement of a loan, and again whenever there is doubt about previously obtained data.

5.1 Individuals

The Company shall obtain and verify name, date of birth, current address, mobile number, a recent photograph, PAN (or Form 97 where permitted), occupation, income and purpose of the loan, together with one Officially Valid Document (OVD): Passport, Driving Licence, proof of possession of Aadhaar number, Voter ID, NREGA Job Card or National Population Register letter. Where the OVD does not show the current address, a deemed OVD permitted under the KYC Directions (such as a recent utility bill) may be accepted, and an updated OVD obtained within the prescribed period.

Income and livelihood evidence shall be proportionate to the loan and risk – for example, land records or KCC for tractor loans, vehicle RCs or transport contracts for commercial vehicle loans, and work orders for construction vehicle loans. The detailed checklist shall be in the Credit Policy.

5.2 Proprietorships and legal entities

For a proprietorship, the proprietor's CDD shall be done as for an individual, together with the business-existence documents prescribed under the KYC Directions. For companies, partnerships, LLPs, trusts, FPOs, cooperative societies and associations, the Company shall obtain constitutional and registration documents, PAN, authorisation, and identity documents of authorised signatories.

5.3 Beneficial ownership

- **Company:** natural person owning more than 10% of shares, capital or profits, or exercising control by other means.
- **Partnership firm:** natural person owning more than 10% of capital or profits, or exercising control by other means.
- **Unincorporated association / body of individuals:** natural person owning more than 15% of property, capital or profits.
- **Trust:** the author, trustees, beneficiaries with 10% or more interest, and any natural person exercising ultimate effective control.

Where no natural person meets these thresholds, the senior managing official shall be treated as the beneficial owner.

5.4 Aadhaar, Digital KYC and V-CIP

- Aadhaar submission shall be voluntary where not mandatory, and Aadhaar shall be verified, masked and stored only as permitted by law. Offline Aadhaar verification (XML/QR) may be used.
- Aadhaar e-KYC authentication through UIDAI may be used only if the Company is notified under the first proviso to Section 11A(1) of the PMLA; the Principal Officer shall confirm this before use.
- Digital KYC and V-CIP shall be carried out only by trained officials, with customer consent, live geo-tagging and time-stamp, liveness checks that do not exclude persons with disabilities, PAN verification with the issuing authority, and data stored in India. A V-CIP account shall become operational only after its concurrent audit is completed. Detailed steps shall be in a separate SOP.

5.5 Third parties and CKYCR

Dealers and DSAs may collect documents but shall not take KYC decisions. Reliance on CDD done by a regulated third party is allowed only as permitted under the KYC Directions; responsibility remains with the Company. KYC records shall be uploaded to and updated on the Central KYC Records Registry (CKYCR) within the timelines prescribed under the KYC Directions and Rule 9 of the PML Rules, and existing CKYCR records may be relied on where current. The KYC Identifier generated by CKYCR shall be communicated to the customer. Where the KYC Identifier is available, the customer shall not be required to resubmit KYC documents, except where there is a change in information, the CKYCR record is incomplete or not as per current norms, the validity of documents has lapsed, or the Company considers it necessary for verification, EDD or risk profiling.

5.6 Outsourcing of KYC-related activities

Where the Company outsources any KYC-related activity (such as sourcing and collection of documents, field or contact point verification, Digital KYC or V-CIP technology, CKYCR uploading, or sanctions-screening and transaction-monitoring tools), it shall do so only in accordance with the RBI directions on managing risks and code of conduct in outsourcing of financial services by NBFCs, the KYC Directions and the Company's Board-approved Outsourcing Policy, as amended from time to time. In particular:

- Decision-making functions of determining compliance with KYC norms, including customer acceptance, risk categorisation and approval of EDD, shall not be outsourced and shall be retained by officials of the Company.
- Outsourcing shall not diminish the Company's obligations. The Company shall remain fully responsible for KYC/AML compliance and for the actions of its service providers, and its accountability to RBI, FIU-IND and customers shall be unaffected.
- Service providers shall be selected after due diligence covering their capability, financial soundness, reputation, conflict of interest and their KYC/AML, data-security and business-continuity controls.
- Every arrangement shall be under a written agreement which, at a minimum, provides for: the scope and service standards; compliance with the KYC Directions, PMLA and PML Rules; confidentiality and security of customer information; no sub-contracting without the Company's prior consent; immediate reporting of suspicious activity to the Principal Officer; the right of the Company, its auditors and RBI to access records and inspect the service provider; business continuity; and termination.
- Customer KYC records collected or processed by the service provider shall belong to the Company, shall be handed over to the Company promptly and shall not be retained or used for any other purpose. Technology outsourcing for V-CIP shall additionally comply with the V-CIP requirements of the KYC Directions, including that data ownership rests with the Company and the service provider retains no data.
- The Company shall monitor the performance of service providers, review each arrangement at least annually, include outsourced KYC activities in its internal audit, and address customer grievances relating to outsourced activities through its grievance redressal mechanism.
- Reliance on CDD done by a regulated third party shall be governed by Section 5.5 and the conditions prescribed in the KYC Directions.

6. ENHANCED DUE DILIGENCE (EDD)

EDD shall apply to High-risk customers, such as those with complex ownership, unexplained source of down payment, frequent profile changes or unusual behaviour. EDD may include additional documents, source-of-funds verification, field investigation, closer monitoring and senior management approval. No relationship shall be established where EDD cannot be completed.

Politically Exposed Persons (PEPs) are individuals entrusted with prominent public functions by a foreign country, along with their family members and close associates. Onboarding or continuing a PEP relationship requires source-of-funds checks, senior management approval and enhanced ongoing monitoring. The Company shall have appropriate risk management systems to determine whether a customer or beneficial owner is a PEP.

Non-face-to-face customers shall be onboarded through V-CIP or Digital KYC with enhanced monitoring. . No service shall be denied solely on account of disability; equivalent alternative channels shall be offered.

7. ASSET AND SELLER VERIFICATION

Before disbursement, the Company shall physically inspect the used vehicle (matching chassis and engine numbers, with geo-tagged photographs), verify registration, ownership, hypothecation and theft flags on VAHAN, verify the seller's identity and authority to sell, obtain NOC and closure proof for any existing finance, and confirm valid insurance and permits. Any discrepancy shall be resolved before disbursement. Detailed procedures shall be in the Credit Policy.

8. MONITORING AND PERIODIC UPDATION

Transactions shall be monitored for consistency with the customer's profile and income. Special attention shall be paid to use of loan funds for other purposes, unexplained foreclosure or cash repayment, repeated financing or resale of the same vehicle, and structuring to avoid thresholds. High-risk accounts shall be monitored more closely.

Special monitoring shall be in place for the following:

- Large and complex transactions with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- Transactions which exceed the thresholds prescribed for specific categories of accounts.
- Transactions in lines to the RBI guideline for the reporting purpose to RBI, FIU-IND etc.
- Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer
- High account turnover inconsistent with the size of the loan or balance maintained, such as frequent prepayments followed by fresh borrowing.
- Repayments through third-party cheques, drafts or accounts, particularly when followed by requests for refund of excess amounts.
- In case unusual operations in any accounts, the matter shall be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.

The Company shall ensure that the extent and frequency of monitoring are commensurate with the risk category assigned to each customer. A system shall be established for reviewing the risk categorisation of customer accounts at least once in every six months, including an assessment of the need to apply Enhanced Due Diligence (EDD) measures. High-risk accounts shall be subjected to more intensive monitoring in accordance with their respective risk profiles.

The Company shall conduct a documented Money Laundering and Terrorist Financing (ML/TF) risk assessment at least annually, covering risks associated with customers, products, services, delivery channels and geographical areas. The findings of such assessment shall be placed before the Board through the Risk Management Committee for review and appropriate action.

The Company shall use a transaction-monitoring system that generates alerts where transactions are inconsistent with the customer's risk category and updated profile. Accounts operated as 'money mules' shall be identified through diligence and monitoring and reported to FIU-IND.

Periodic updation of KYC: The Company shall follow a risk-based approach and carry out periodic updation of KYC at least once in every two years for High-risk, once in every eight years for Medium-risk and once in every ten years for Low-risk customers, from the date of opening of the account or last KYC updation. For Low-risk individual customers, all transactions shall be allowed and KYC shall be updated within one year of its falling due (or such later date as permitted under the KYC Directions), with such accounts kept under regular monitoring.

- **Individuals – no change:** a self-declaration shall be obtained through the registered email-id, registered mobile number, digital channels (including the Company's mobile application), letter, etc.
- **Individuals – change in address only:** a self-declaration of the new address shall be obtained through the above channels, together with a copy of the OVD or deemed OVD (or the equivalent e-document) as proof

of the new address, and the address shall be verified through positive confirmation (address verification letter, contact point verification, deliverables, etc.) within two months.

- **Aadhaar OTP e-KYC:** may be used in non-face-to-face mode for updation, provided the mobile number used for Aadhaar authentication is the same as that registered with the Company. A declared current address different from the Aadhaar address shall not then require positive confirmation.
- **Customers other than individuals:** where there is no change, a self-declaration shall be obtained through the registered email-id, digital channels, a letter from an authorised official or a board resolution, and beneficial ownership information shall be verified and updated; where there is a change, KYC equivalent to onboarding a new legal entity customer shall be carried out.
- **Additional measures:** KYC documents shall be brought to current CDD standards, and fresh KYC done where the documents have expired; PAN shall be verified with the issuing authority; an acknowledgement mentioning the date of receipt shall be given to the customer, and after updation of the records (including CKYCR) an intimation mentioning the date of updation shall be sent; and customers may update KYC at any branch of the Company. Customers who were minors at account opening shall submit fresh photographs and current CDD documents on becoming major.
- **Exceptional measures:** the Company does not prescribe any additional or exceptional measures for updation (such as a recent photograph, physical presence, updation only at the home branch or a more frequent periodicity) beyond those stated above.
- **Due notices:** at least three advance intimations before the due date, and at least three reminders after the due date to customers who have not complied, each including at least one by letter, shall be given at appropriate intervals. These shall contain easy-to-understand instructions, the escalation mechanism and the consequences of non-updation, and their issue shall be recorded in the system against each customer for audit trail.
- **Customer obligation:** customers shall be advised to submit any update in their KYC documents to the Company within 30 days of such update.
- **PAN / Form No. 97 of existing customers:** where the PAN or Form No. 97 (or the corresponding form under the Income-tax law in force) of an existing customer is not obtained by the date notified by the Central Government, operations in the account shall be temporarily ceased (in loan accounts, only credits shall be allowed), after giving the customer an accessible notice and a reasonable opportunity of being heard. Customers unable to provide these owing to injury, illness, infirmity on account of old age or similar causes may continue to be serviced, subject to enhanced monitoring.

9. SANCTIONS SCREENING

Customers, beneficial owners, co-borrowers, guarantors and authorised signatories shall be screened against the UN Security Council sanctions lists and the lists designated under the UAPA and the WMD Act, at onboarding and whenever the lists are updated. Where a match is found or suspected, the Company shall not carry out the transaction, shall freeze the assets concerned, and shall report to the Central and State Nodal Officers and FIU-IND as prescribed under Section 51A of the UAPA (with intimation to the Ministry of Home Affairs), Section 12A of the WMD Act (with a copy to RBI) and the KYC Directions. The Principal Officer shall maintain a procedure recording the current lists, frequency and reporting timelines.

10. REPORTING TO FIU-IND

- The Company shall file STRs, Cash Transaction Reports, Counterfeit Currency Reports and Non-Profit Organisation Transaction Reports, as applicable, electronically and within the timelines under Rule 7 of the PML Rules. The Principal Officer shall maintain a reporting calendar.
- An STR shall be filed even if the transaction was only attempted or not completed. Filing an STR shall not by itself restrict the account.
- **No tipping-off:** no one shall disclose to the customer that an STR has been or may be filed. If completing CDD would tip off a suspected customer, CDD shall not be pursued and an STR shall be filed.

11. RECORD KEEPING

Transaction records shall be kept for at least five years from the date of transaction, and KYC records for at least five years after the relationship ends, in a form that is retrievable and can be produced to authorities on request. Customer information shall be kept confidential and used only as permitted by law. Transaction records shall contain sufficient detail (nature, amount and currency, date and parties) to permit reconstruction of individual transactions.

12. TRAINING, AGENTS AND AUDIT

- Employees shall be screened at recruitment and trained on KYC/AML at induction and periodically, with focus on field and credit staff. Wilful negligence shall attract disciplinary action.
- Dealers, DSAs and service providers shall be bound by contract to KYC/AML obligations and subject to audit.
- Customers shall be informed, in simple language, that identity verification is required by law.
- New products or technologies shall be assessed for ML/TF risk before launch.

13. REGULATORY OVERRIDE AND REVIEW

Where any law or RBI direction differs from this Policy, the law or direction shall prevail. This Policy shall be reviewed by the Board at least once every financial year, or earlier on a change in law or in the Company's business. The Principal Officer shall report to the Board at least annually on the functioning of the KYC/AML framework, including FIU-IND reports, periodic updation status, training and audit findings.

ANNEXURE – ILLUSTRATIVE RED FLAGS

- Refusal to provide identity documents or explain source of funds.
- Down payment funded by an unrelated third party without explanation.
- Cash repayments or early closure inconsistent with declared income.
- Tampered chassis or engine numbers, duplicate or recently re-issued RCs, or unexplained re-registration in another State.
- Vehicle price far above or below assessed value, or related-party sales designed to extract cash.
- Attempts to influence staff to bypass KYC or not to report.

— **End of Policy** —