BHAWANA CAPITAL PRIVATE LIMITED

KYC – AML – CFT POLICY

Know Your Customer, Anti-Money Laundering and Combating the Financing of Terrorism

1. Introduction and Regulatory Basis

Bhawana Capital Private Limited ("the Company") is a non-deposit-taking Non-Banking Financial Company – Base Layer registered with the Reserve Bank of India ("RBI"). This Policy is adopted in compliance with the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, as amended from time to time ("the KYC Directions"), the Prevention of Money-Laundering Act, 2002 ("PMLA"), the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended ("the PML Rules"), the Unlawful Activities (Prevention) Act, 1967 ("UAPA") and the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act").

The objectives of this Policy are to enable the Company to know and understand its customers and their financial dealings, to manage money-laundering and terrorist-financing risks prudently, and to prevent the Company from being used, intentionally or otherwise, for money laundering, terrorist financing or other unlawful activity.

2. Applicability

This Policy prevails over any contrary instruction in any document, process or circular of the Company relating to KYC / AML / CFT, and applies to all existing and future products and business verticals. Where customers are sourced or serviced through a Loan Service Provider ("LSP") or Digital Lending App, the Company remains fully and ultimately responsible for compliance with this Policy and with all applicable KYC, AML and CFT requirements.

3. Key Definitions

- **Customer Due Diligence (CDD)** – identifying and verifying the customer and, where applicable, the beneficial owner, using reliable and independent sources of data or information.
- **Officially Valid Document (OVD)** – the passport, the driving licence, proof of possession of Aadhaar, the Voter Identity Card, the NREGA job card duly signed by an officer of the State Government, or the letter issued by the National Population Register containing details of name and address.
- **Digital KYC** – capturing a live photograph of the customer along with the OVD or proof of possession of Aadhaar, and the latitude and longitude of the location of capture, by an authorised officer of the Company.
- **V-CIP (Video-based Customer Identification Process)** – a consent-based, real-time audio-visual interaction with the customer, undertaken by an authorised official, which is treated as face-to-face for the purposes of this Policy.
- **Beneficial Owner** – the natural person who ultimately owns or controls a customer, or on whose behalf a transaction is conducted, determined in accordance with the PML Rules.
- **Politically Exposed Person (PEP)** – an individual who is or has been entrusted with a prominent public function by a foreign country, including heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.
- **KYC Identifier** – the unique number or code assigned to a customer by the Central KYC Records Registry ("CKYCR").

4. Elements of the Policy

The Company's KYC-AML-CFT framework comprises four elements: the Customer Acceptance Policy; the Customer Identification Procedure; Monitoring of Transactions; and Risk Management.

4.1 Customer Acceptance Policy

- No account is opened and no disbursal is made in an anonymous, fictitious or benami name.

- A customer is accepted only after successful CDD. Where CDD cannot be completed — for example owing to non-cooperation of the customer or the unreliability of documents or information — the relationship is not established, and the case is considered for filing a Suspicious Transaction Report.
- No account-based relationship or transaction is undertaken without following the CDD procedure.
- Mandatory KYC information is obtained at onboarding and at periodic updation; optional information is obtained only with the explicit consent of the customer.
- The identity of the customer is screened against the sanctions and designated lists referred to in Section 9 before any account-based relationship is established, and thereafter on an ongoing basis.
- These safeguards are applied so as not to cause harassment to genuine customers, nor to unduly restrict access to services for financially or socially disadvantaged segments.

4.2 Customer Identification Procedure

Customer identification entails carrying out CDD using reliable and independent source documents, data or information, and understanding the intended nature of the relationship. Identification is undertaken at the commencement of an account-based relationship, whenever there is doubt about the authenticity or adequacy of previously obtained data, and while carrying out transactions. Each customer is allotted a Unique Customer Identification Code (UCIC).

4.3 Monitoring of Transactions

Ongoing monitoring is carried out on a risk-sensitive basis to identify activity outside the normal or expected pattern, with enhanced attention to complex or unusually large transactions and to transactions with no apparent economic or lawful purpose. High-risk accounts are subjected to intensified monitoring and periodic review of risk categorisation.

4.4 Risk Management and Risk Categorisation

Customers are categorised as Low, Medium or High risk on a risk-based approach, considering the customer's identity, social and financial status, nature of activity, mode of onboarding, source of funds, repayment behaviour and other relevant factors, and subject to the categorisation mandated for non-face-to-face onboarding under Section 5. Risk categorisation is reviewed periodically, is treated as confidential and is not disclosed to the customer.

5. Customer Due Diligence

For an individual customer, the Company carries out CDD through its digital platform in accordance with the KYC Directions. This comprises: verification of the Permanent Account Number; obtaining an Officially Valid Document, including through offline verification of Aadhaar or an equivalent e-document retrieved from the customer's DigiLocker account; and capturing a live photograph of the customer, which is subjected to a liveness check and matched against the photograph on the document.

- Aadhaar numbers are redacted or masked as required under the Aadhaar Act, and no unmasked Aadhaar number is retained.
- Equivalent e-documents, e-Aadhaar and documents retrieved from the customer's DigiLocker account are accepted to the extent permitted by the KYC Directions.
- Where Digital KYC or V-CIP is used, it is carried out with the safeguards prescribed by RBI, including liveness detection, face matching, secure storage of the record and operation by trained officials.
- Where account opening through OTP-based e-KYC in non-face-to-face mode is used, it is undertaken only subject to the conditions and limits prescribed by RBI, and such accounts are subjected to full CDD within the period prescribed.
- Where the customer is acting on behalf of another person or entity, the identity of the beneficial owner is also established and verified.

Non-face-to-face onboarding. Where CDD is completed in non-face-to-face mode (other than through V-CIP, which is treated as face-to-face), the Company applies the safeguards prescribed for non-face-to-face customer onboarding, including verification of the Permanent Account Number from the database of the issuing authority, verification of the customer's mobile number and contact details, and disbursal of the first credit into the borrower's own verified bank account. Customers onboarded in non-face-to-face mode are categorised as High risk and subjected to enhanced monitoring until their identity is verified in a face-to-face

manner or through V-CIP. The form of enhanced due diligence and monitoring applied to such customers is laid down in the operating procedures approved under this Policy.

Where CDD processes are executed through a technology service provider or an LSP on the Company's behalf, the Company remains fully and ultimately responsible for the CDD so performed (see Section 15).

6. Enhanced Due Diligence and Politically Exposed Persons

Enhanced Due Diligence is applied to customers categorised as High risk, and includes obtaining additional information on the source of funds and the purpose of the relationship, and more frequent monitoring and review.

Where a customer or beneficial owner is, or subsequently becomes, a Politically Exposed Person or a relative or close associate of one, the relationship is established or continued only with the approval of senior management, the source of funds is established, and the account is subjected to enhanced ongoing monitoring.

Enhanced Due Diligence is also applied where the customer is from, or the transaction involves, a jurisdiction identified as high risk or as having strategic AML/CFT deficiencies.

7. Periodic Updation of KYC

The Company carries out periodic updation of KYC records on a risk-based basis, in accordance with the timelines prescribed by RBI — presently at least once every two years for High-risk customers, once every eight years for Medium-risk customers and once every ten years for Low-risk customers, from the date of opening of the account or the last KYC updation. Where there is no change in the KYC information, a self-declaration from the customer is sufficient; where only the address has changed, a self-declaration of the new address is obtained and verified within the prescribed period. Customers are given advance intimation of the requirement for periodic updation.

8. Central KYC Records Registry and FATCA / CRS

The KYC records of customers are uploaded to the CKYCR within the timelines prescribed under the PML Rules, and are updated whenever there is a change. Where a customer submits a KYC Identifier, the Company retrieves the KYC records online from the CKYCR and does not require the customer to submit KYC documents afresh, unless there is a change in the information on record, the record is incomplete or invalid, or the validity of the record has lapsed. Where KYC records are downloaded from the CKYCR, the Company is not required to re-verify the identity or address of the customer where the downloaded records are current and compliant with the PMLA and the PML Rules; all other aspects of the CDD procedure remain the responsibility of the Company.

The Company complies with FATCA and CRS reporting obligations to the extent it constitutes a Reporting Financial Institution under Rules 114F to 114H of the Income-tax Rules, 1962.

9. Screening against Sanctions and Designated Lists

The Company screens customers and beneficial owners, at onboarding and on an ongoing basis, against the lists of individuals and entities designated under Sections 35 and 51A of the UAPA (including the United Nations Security Council lists), and against any other list circulated by RBI or the Government of India. The Company likewise implements, without delay, orders issued under Section 12A of the WMD Act, including the freezing, unfreezing and prohibition of transactions involving designated persons.

Where a match is found, the Company does not establish the relationship or carry out the transaction, freezes the funds and assets as required, and reports the matter without delay to the prescribed authorities and to FIU-IND.

10. Principal Officer

The Company designates a Principal Officer, of sufficient seniority, who is responsible for monitoring and reporting of transactions and for sharing of information under the PMLA, and who liaises with enforcement and other agencies. The name, designation and address of the Principal Officer are communicated to FIU-IND and to RBI.

11. Designated Director

The Board nominates a Designated Director who is responsible for ensuring overall compliance with the obligations imposed under the PMLA and the PML Rules. The Principal Officer is not nominated as the Designated Director. The details of the Designated Director are communicated to FIU-IND.

12. Reporting to FIU-IND

Under Section 12 of the PMLA read with the PML Rules, the Company furnishes the prescribed reports to the Director, Financial Intelligence Unit – India:

- Cash and other prescribed transaction reports are furnished by the 15th day of the succeeding month.
- Suspicious Transaction Reports are furnished promptly, and in any case not later than seven working days from the date of establishing suspicion, whether or not the transaction was completed.
- Where there is reason to believe that transactions have been structured below a reporting threshold to evade reporting, such information is also furnished.
- Strict confidentiality is maintained in relation to the reporting of suspicious transactions, and no customer is tipped off. NIL reports are not required where there is no reportable transaction in the relevant period.

13. Maintenance and Preservation of Records

Records of transactions are maintained for at least five years from the date of the transaction. Records of the identity and address of customers, and the CDD records, are maintained for at least five years after the business relationship ends or the account is closed, whichever is later. Records are maintained in a manner that permits their retrieval and reconstruction, and their production to competent authorities, without delay.

14. Money Laundering and Terrorist Financing Risk Assessment

The Company carries out and documents a periodic assessment of its money-laundering and terrorist-financing risk, taking into account its customers, products, delivery channels, geographies and the use of new technologies. The outcome of the assessment is placed before the Board, and a risk-based approach guides the allocation of resources and the design of controls.

15. Reliance on Third Parties; LSP and Service-Provider Arrangements

15.1 Statutory reliance. The Company may rely on customer due diligence carried out by a third party that is itself a regulated entity, subject to the conditions prescribed under the PML Rules and the KYC Directions: the CDD records or information are obtained from the third party or from the CKYCR within the prescribed period; the third party undertakes to make the underlying identification data and documents available to the Company without delay on request; the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements, and is not based in a jurisdiction identified as high risk; and the ultimate responsibility for CDD and enhanced due diligence remains with the Company.

15.2 LSP and service-provider arrangements. Where onboarding or CDD processes are executed through an LSP or a technology service provider, such provider acts solely as the Company's agent. The decision to accept a customer and the determination of compliance with KYC norms are not outsourced; all KYC records are held in, and available to, the Company's systems; and the Company retains audit and inspection rights over the provider's KYC processes. The Company remains fully and ultimately responsible for CDD irrespective of such arrangements.

16. Group-wide AML / CFT Programme

As part of a financial group, the Company implements group-wide programmes against money laundering and terrorist financing, including policies on sharing information within the group for CDD and ML/TF risk-management purposes, subject to safeguards on confidentiality and use of the information exchanged and to applicable Indian law. The statutory roles of the Designated Director and the Principal Officer vest in the Company and are not delegated within the group.

17. Employee Screening, Training and Awareness

The Company applies appropriate screening at the time of hiring employees who have access to customer information or to AML/CFT processes. Employees, and the staff of LSPs and agents who interact with customers, receive ongoing training on KYC, AML and CFT obligations, on the identification and reporting of suspicious transactions and on the prohibition against tipping off, calibrated to the role of the person concerned.

18. Internal Audit and Compliance Review

Compliance with this Policy and with the applicable KYC / AML / CFT requirements is reviewed independently through the Company's internal audit function, and the findings and the status of remediation are placed before the Board or the Audit Committee. Any new technology or process adopted for customer onboarding is reviewed before it is operationalised.

19. Confidentiality

Information collected from customers for the purpose of KYC is treated as confidential and is not disclosed for any other purpose, including cross-selling, without the express consent of the customer, save where disclosure is required by law or by a competent authority.

20. Review

This Policy is reviewed by the Board of Directors at least annually, and whenever required by a change in the applicable RBI Directions, the PMLA, the PML Rules or the guidance issued by FIU-IND. In the event of any inconsistency, the applicable RBI Directions, the PMLA and the PML Rules prevail over this Policy.