

ITI Gold Loans Limited

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

Policy Title	Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy
Regulatory Basis	RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 [RBI/DOR/2025-26/361, DOR.AML.REC.No.280/14.01.003/2025-26 dated November 28, 2025, updated as on December 29, 2025], read with the Prevention of Money-Laundering Act, 2002, the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, and the RBI (NBFC – Know Your Customer) Amendment Directions, 2025
Version	5.0
Approved By	Board of Directors
Effective Date	15 th April, 2026
Policy Owner	Principal Officer (AML/CFT) / Company Secretary & Compliance Officer
Review Frequency	Annually, or earlier upon regulatory change

1. Preamble and Objective

This Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy (“the Policy”) is framed by [ITI Gold Loans Limited] (“the Company”) in compliance with the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 dated November 28, 2025, as updated on December 29, 2025 (“the KYC Directions”), which repealed and replaced the erstwhile Master Direction – Know Your Customer (KYC) Direction, 2016 as applicable to NBFCs. The Policy is further anchored in the Prevention of Money-Laundering Act, 2002 (“PML Act”), the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (“PML Rules”), and India’s commitments as a member of the Financial Action Task Force (FATF).

The objective of this Policy is to:

- Prevent the Company from being used, intentionally or unintentionally, as a conduit for money laundering (ML) or terrorist financing (TF) activities;
- Enable the Company to know and understand its customers and their financial dealings, so as to manage risks prudently;
- Put in place appropriate controls for detecting and reporting suspicious activities in accordance with applicable laws and RBI directions; and
- Ensure compliance with the four key elements prescribed under the KYC Directions:
 - (i) Customer Acceptance Policy, (ii) Risk Management, (iii) Customer Identification Procedure (CIP) and (iv) Monitoring of Transactions.

2. Applicability

This Policy applies to all categories of customers, products, and services of the Company across its gold loans and to all employees and officers, business correspondents, and other persons engaged in customer onboarding or transaction processing on the Company’s behalf. It extends, to the extent applicable, to any branches of the Company.

3. Definitions

- **“Customer Due Diligence (CDD)”** means identifying and verifying the customer and the beneficial owner, using reliable and independent documents, data, or information.
- **“Beneficial Owner (BO)”** means the natural person(s) who ultimately own, control, or exercise significant control over a customer, and/or the natural person on whose behalf a transaction is being conducted; determined per the ownership/control/senior-managing-official thresholds prescribed under the KYC Directions and the PML Rules.
- **“Officially Valid Document (OVD)”** means the documents prescribed under the PML Rules for proof of identity/address (e.g., Aadhaar, passport, voter ID, driving licence, NREGA job card, or such other document as notified by the Central Government).
- **“Politically Exposed Persons (PEPs)”** means individuals who have been entrusted with prominent public functions in a foreign country, including heads of state/government, senior politicians, senior government/judicial/military officials, senior executives of state-owned corporations, and important political party officials.

- **“Principal Officer”** means the officer nominated by the Company, responsible for ensuring compliance, monitoring transactions, and reporting to the Financial Intelligence Unit – India (FIU-IND).
- **“Designated Director”** means the Director designated by the Board to ensure overall compliance with the obligations under the PML Act and Rules.
- **“Suspicious Transaction”** means a transaction, whether or not made in cash, which gives rise to reasonable grounds of suspicion of involving proceeds of crime, or appears to be made in circumstances of unusual or unjustified complexity, or which does not have an economic rationale or bona fide purpose.
- **“Central KYC Records Registry (CKYCR)”** means the centralised repository maintained by CERSAI for storing, safeguarding and retrieving KYC records of customers.

4. Key Elements of the KYC Policy

In line with the KYC Directions, this Policy is built around four key elements:

- Customer Acceptance Policy (CAP)
- Risk Management
- Customer Identification Procedure (CIP)
- Monitoring of Transactions

5. Customer Acceptance Policy

The Company shall:

- Not open an account or establish a relationship in anonymous or fictitious/benami name(s);
- Not open an account where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the information/documents furnished and shall consider filing a Suspicious Transaction Report where warranted;
- Not establish a relationship until the identity of a new customer is verified and as necessary, the source of funds ascertained;
- Apply CDD at the level appropriate to the nature of the business relationship and the perceived risk, ensuring that the Company does not open accounts that could unduly delay or deny access to financial services to persons who are financially or socially disadvantaged;
- Document, and provide reasons in writing, for the rejection of any application for account opening or periodic KYC updation, in line with the RBI (NBFC – Know Your Customer) (2nd Amendment) Directions, 2025 mandating that no such rejection may be automated without a recorded, reasoned justification by an authorised officer;
- Ensure that persons with disabilities are not denied access to the Company's products or services solely on the basis of an automated digital verification failure, and provide alternate, assisted verification channels where required.

6. Risk Management and Customer Risk Categorisation

The Company shall adopt a risk-based approach and categorise customers as Low, Medium, or High risk, having regard to parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and location.

6.1 Low-Risk Customers

Individuals (other than High Net-Worth) and entities whose identities and sources of wealth can be easily identified, and whose transactions largely conform to the known profile, may be categorised as low risk, subject to simplified due diligence measures.

6.2 High-Risk Customers / Enhanced Due Diligence (EDD)

EDD shall be applied to customers assessed as high risk, including but not limited to: non-resident customers, PEPs and their family members/close associates, legal persons/arrangements with complex ownership structures, non-face-to-face customers, and customers in businesses assessed as vulnerable to money laundering (e.g., cash-intensive businesses). EDD measures shall include obtaining senior management approval for establishing the relationship, ascertaining source of funds/wealth, and conducting enhanced ongoing monitoring.

6.3 Group / Combined Risk Assessment

The Company's overall risk assessment shall have regard to country/geographical risk, customer risk, and product/service/delivery-channel risk, and shall be periodically reviewed and updated, including on account of any changes to national or supra-national risk assessments.

7. Customer Identification Procedure (CIP)

The Company shall undertake identification of customers in the following manner, in a suitable manner as prescribed under Chapter V of the KYC Directions:

7.1 Individuals

- Obtain one certified copy of an OVD (or e-KYC/Aadhaar Offline Verification/Digital KYC, as permitted) containing details of identity and address, one recent photograph, and PAN or Form 60 where PAN is not available;
- Where Aadhaar-based authentication/offline verification is used, the Company shall ensure the customer's informed consent, and Aadhaar shall not be treated as mandatory where alternate OVDs are offered;
- A self-attested photograph shall be obtained from the customer;
- PAN details furnished shall be verified against the details available with the issuing authority, and the same shall be verified from the database maintained by relevant authorities.

7.2 Sole Proprietary Firms

In addition to the individual CDD applicable to the proprietor, any two of the following documents (or such other documents as may satisfy the Company as to the existence of the firm) shall be obtained: registration certificate, certificate/licence issued by the municipal authorities under the Shops and Establishments Act, GST registration certificate, sales/income tax returns, CST/VAT/GST certificate, IEC issued to the proprietary concern, complete

Income Tax Return (not just acknowledgement) in the name of the proprietor, and utility bills such as electricity, water, or landline telephone bills in the name of the proprietary concern.

7.3 Legal Entities (Companies, Partnership Firms, Trusts, etc.)

- Verification of the legal status of the entity through certificate of incorporation/registration, Memorandum and Articles of Association (or partnership deed/trust deed, as applicable), and the registered office and principal place of business, if different;
- Identification and verification of persons holding senior management positions and those authorised to act on behalf of the entity, along with the relevant power of attorney/Board resolution;
- Obtaining PAN, or Form No. 60 for an unincorporated association or body of individuals (which, for this purpose, includes societies).

7.4 Identification of Beneficial Owner

For legal person customers, the Company shall identify the natural person(s) who ultimately own or control the customer through ownership or control, applying the threshold prescribed under the PML Rules (ownership of/entitlement to a specified percentage of shares, capital, or profits, or control through other means). Where no natural person is identified under the ownership/control test, the beneficial owner shall be the relevant natural person holding the position of senior managing official.

7.5 On-going Due Diligence

The Company shall exercise ongoing due diligence with respect to the business relationship, and closely examine transactions to ensure they are consistent with the Company's knowledge of the customer, its business, and risk profile. Particular attention shall be given to indicators such as high account turnover inconsistent with the size of the balance maintained, and deposit of third-party cheques, drafts, or other instruments in existing or newly opened accounts, followed by ATM/withdrawal transactions inconsistent with the customer's declared profile.

8. Periodic Updation of KYC

The Company shall carry out periodic updation of KYC records at intervals commensurate with customer risk category – not exceeding two years for high risk, eight years for medium risk, and ten years for low risk customers, unless a shorter period is warranted. In respect of low-risk customers specifically, and in line with the RBI's June 2025 customer-centric KYC amendment to paragraph 38 of the erstwhile Direction (carried forward under the current framework), such customers shall have time until one year from their KYC due date, or June 30, 2026, whichever is later, to complete the periodic updation, with all transactions on such accounts remaining under regular monitoring during this period.

Where a customer is due for re-KYC, the Company shall issue at least three advance intimations (at least one by letter) prior to the due date, and, in case of continued non-compliance after the due date, at least three further reminders including one by letter, before considering any restriction on the account.

9. Central KYC Records Registry (CKYCR)

The Company shall upload the KYC data of all individual accounts opened on or after the applicable date to the CKYCR, in the prescribed format, within the timelines specified by the RBI/CERSAI. Where the Company downloads and relies on KYC records from the CKYCR, the following shall apply, pursuant to the RBI (NBFC – Know Your Customer) Amendment Directions, 2025:

- The regulated entity that last uploaded or updated the customer's KYC records in the CKYCR shall be responsible for verifying the identity and/or address of the customer;
- Accordingly, the Company, upon downloading and relying on such CKYCR records, shall not be required to re-verify the authenticity of the customer's identity and/or address, provided the downloaded records are current and compliant with the PML Act/Rules;
- Notwithstanding the above, the Company shall remain responsible for all other aspects of the CDD process and its obligations under this Policy and the KYC Directions.

10. Record Management

- The Company shall maintain records of all transactions, including cash transactions above the prescribed threshold, in a manner that permits reconstruction of individual transactions;
- Records of identification data (obtained through CDD) and account files/business correspondence shall be preserved for at least five years after the business relationship has ended, or the date of the occasional transaction, as applicable;
- Records evidencing the identity of customers and beneficial owners, and account files, shall be made available to competent authorities upon request, within the prescribed timelines.

11. Reporting to the Financial Intelligence Unit – India (FIU-IND)

The Company, through its Principal Officer, shall furnish the following reports to FIU-IND within the timelines prescribed under the PML Rules:

- Cash Transaction Reports (CTR) – for all cash transactions of value exceeding the prescribed threshold, and integrally connected cash transactions;
- Suspicious Transaction Reports (STR) – within seven working days of establishing suspicion, irrespective of the transaction amount, without informing the customer ('no tipping-off');

Employees and officers of the Company shall be strictly prohibited from disclosing ('tipping off') to the customer, or any third party, the fact that an STR or related information is being or has been reported to FIU-IND.

12. Governance – Principal Officer and Designated Director

- The Board shall designate a Principal Officer, of a sufficiently senior level, responsible for monitoring and reporting all transactions and information under this Policy, and for coordinating compliance with FIU-IND, RBI, and other authorities;
- The Board shall also designate a Director as the Designated Director, responsible for overall compliance with the obligations under the PML Act, PML Rules, and this Policy;
- An internal control framework, including a compliance function and independent audit function, shall be maintained to test the adequacy of AML/CFT controls.

13. Screening Against Sanctions Lists

The Company shall screen prospective and existing customers against the lists circulated by the RBI and the Government of India under the Unlawful Activities (Prevention) Act, 1967 (UAPA), including the UN Security Council's consolidated sanctions lists, and shall not establish or continue a relationship, or process a transaction, where a match is confirmed, except as permitted by applicable directions. Any such match or attempted transaction shall be reported to FIU-IND and relevant authorities without delay.

14. New Products

Prior to the launch of new products, business practices, or delivery mechanisms the Company shall undertake a money-laundering/terrorist-financing risk assessment and put in place appropriate mitigating measures.

15. Employee Training and Awareness

The Company shall have an ongoing training programme for employees, including new joiners, front-line staff, covering CDD requirements, red flags for suspicious transactions, and reporting obligations, so that personnel are adequately trained in KYC/AML/CFT procedures.

16. Review of the Policy

This Policy shall be reviewed by the Board at least annually, or earlier upon any change in the KYC Directions, the PML Act/Rules, or FATF standards, or pursuant to observations from RBI supervisory inspections. A compliance status report shall be placed before the Board (or the Audit Committee/Risk Management Committee, as applicable) at regular intervals.

Annexure A – Illustrative List of Officially Valid Documents (OVDs)

- Passport
- Aadhaar (subject to offline verification/e-KYC consent; not mandatory where an alternate OVD is offered)
- Voter's Identity Card issued by the Election Commission of India
- Driving Licence
- Job Card issued by NREGA, duly signed by a State Government officer
- Letter issued by the National Population Register containing details of name and address
- Any other document notified by the Central Government in consultation with the Regulator