



INDUSTRIAL INVESTMENT TRUST LIMITED

KYC AND ANTI MONEY LAUNDERING POLICY

Industrial Investment Trust Limited
CIN: L65990MH1933PLC001998
Regd. Off: 101A, The Capital, G-Block,
Plot no.C-70 Bandra Kurla Complex,
Bandra (East) Mumbai Mumbai City
MH 400051
Website: www.iitlgroup.com

Version	Date of Approval/ Review
V.1	04/03/2023
V.2	06/08/2025
V.3	05/08/2026
Recommended By	CEO – NBFC
Approved By	Board of Directors

1. INTRODUCTION

Industrial Investment Trust Limited (IITL) is committed to conducting its lending and investment activities in compliance with the Reserve Bank of India's (RBI) Master Directions on KYC and AML (updated as on 12th June 2025). IITL ensures alignment with the Prevention of Money Laundering Act (PMLA) and international standards set by the Financial Action Task Force (FATF).

This KYC & AML policy of IITL is approved by the Board of Directors, this policy is applicable to all products and services offered by IITL across all its offices.

2. OBJECTIVE

The objective of this Policy is to standardize KYC documentation across IITL and to lay down clear guidelines to prevent the Company from being used for money laundering activities.

This Policy serves to:

- Protect the Company from being used intentionally or unintentionally by criminal elements for money laundering/ fraudulent/anti-social activities
- Protect the Company from being used intentionally or unintentionally by criminal elements for money laundering/ fraudulent/anti-social activities
- Define and implement Customer Identification Procedures (CIP), Customer Due Diligence (CDD), and Enhanced Due Diligence (EDD) based on risk
- Prevent the Company from being used for laundering of proceeds from criminal activities or financing of terrorism
- Promote a clear understanding of the customer's background, business model, and financial behaviour, helping IITL assess credit and compliance risks prudently
- Ensure reporting of suspicious activities to designated authorities (e.g., FIU-IND) as per regulatory timelines
- Adopt appropriate standards and RBI guidelines related to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT)

This Policy applies to all categories of customers, including individuals, partnership firms, companies, trusts, societies, and other legal entities, as well as to their authorized representatives, agents, or third parties acting on their behalf.

3. APPLICABILITY & EFFECTIVE DATE

This Policy shall govern all KYC, Customer Due Diligence (CDD), and Anti-Money Laundering (AML) practices applicable to all lending and investment activities undertaken by IITL. It is binding on all teams, systems, and customer touchpoints where client identification, onboarding, verification, or ongoing due diligence is conducted.

This policy applies to all our customers—individuals, firms, companies, trusts, and other legal entities—as well as beneficial owners and anyone authorised to act on their behalf.

This Policy comes into force from the date of its initial approval by the Board of Directors. Any future revisions, modifications, or updates shall be deemed effective from the date of approval by the Board.

It is the responsibility of every employee and designated official of IITL to implement this Policy in both letter and spirit. Queries, exceptions, or clarifications must be directed to the Compliance Function for resolution.

4. KEY ELEMENTS

IITL's KYC-AML framework is guided by the four foundational pillars outlined by RBI's Master Directions:

i) Customer Identification Procedure (CIP)

Covers the process of identifying and verifying the identity of customers at the time of establishing a relationship and on an ongoing basis.

This includes:

- Identification of the customer
- Identification and verification of the Beneficial Owner (BO) in the case of entities
- Verification of authorized signatories and persons acting on behalf of the customer
- Use of officially valid documents (OVDs) or other prescribed mechanisms

ii) Customer Acceptance Policy (CAP)

Lays down the criteria for accepting customers, ensuring that no account is opened in anonymous or fictitious names, and outlines the types of customers that may be refused based on risk and documentation.

iii) Risk Management

Framework to classify customers into risk categories (High, Medium, Low) based on factors such as nature of business, source of funds, geography, and transaction profile. Appropriate due diligence (CDD/EDD) is applied accordingly.

iv) Monitoring of Transactions

Ongoing monitoring of customer transactions to identify unusual patterns or suspicious activity. This includes generation of alerts, review of high-risk accounts, and filing of Suspicious Transaction Reports (STRs), where necessary.

5. COMPLIANCE OF KYC POLICY

IITL shall ensure compliance with this Policy through:

- **Senior Management Team Oversight** for the compliance of KYC Policy. The Senior Management Team includes the Chairman, Managing Director (MD), Chief Executive Officer (CEO), and such other officials as may be designated from time to time for the purpose of KYC compliance.
- **Defined responsibility allocation** across departments to ensure effective implementation of KYC-AML procedures in day-to-day operations.

- **Independent evaluation** of compliance with this Policy, including regulatory requirements.
- **Internal audit system** to verify implementation of KYC–AML procedures at various stages such as onboarding, monitoring, and record-keeping.
- **Submission of quarterly audit and compliance reports** to the Audit Committee of the Board for review and necessary guidance.
- **Decision-making functions related to KYC** compliance shall not be outsourced. All such decisions shall rest solely with authorised officials of IITL and shall not be delegated to any external vendors or third-party service providers.
- **Periodic staff training** to ensure awareness and proper implementation of KYC & AML procedures, including customer onboarding, risk categorisation, monitoring, and reporting.

DEFINITIONS

The terms used and not defined in this Policy shall have the same meaning as assigned to them in the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016, as amended from time to time.

- i. **“Act” and “Rules”** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.
- ii. **“Authentication”**, in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, as amended from time to time.
- iii. **Beneficial Owner (BO):**
 - a. Where the customer is a **Company**, the BO would be the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.
Explanation: “Controlling ownership interest” means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.
Explanation 2: “Control” shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.
 - b. Where the customer is a **partnership firm**, the BO is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership
 - c. Where the customer is an **unincorporated association or body of individuals**, the BO is the natural person(s), who, whether acting alone or together, or through

one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified in any of the above non-individual entities, the BO is the relevant natural person who holds the position of senior managing official.

- d. Where the customer is a **Trust**, the identification of BO shall include identification of the author of the trust, the trustee, the beneficiaries with 10 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.
- iv. **Digital KYC:** means capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, 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 Regulated Entity (RE) as per the provisions contained in the Act.
- v. **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
- vi. **Group:** The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961 (43 of 1961).
- vii. **Officially Valid Document ("OVD"):** means the passport, the driving licence, proof of possession of Aadhaar number, the 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 and letter issued by the National Population Register containing details of name and address.

Provided that:

- a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
- b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:
 - i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill),
 - ii. property or Municipal tax receipt,
 - iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address,
 - iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial

- banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.
- c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above.
- d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

- viii. **Politically Exposed Persons (PEPs):** are individuals who are or have been entrusted with prominent public functions by a foreign country including the Heads of States/ Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations, important political party officials.
- ix. **Video based Customer Identification Process (V-CIP):** an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face customer identification process.

Customer Acceptance Policy (CAP)

In line with regulatory requirements and prudent credit practices, IITL's Customer Acceptance Policy (CAP) lays down the guiding principles for onboarding borrowers, guarantors, and other associated parties. The purpose of this policy is to ensure transparency, traceability, and full compliance with KYC-AML obligations during customer onboarding and relationship management.

1. Objectives

- To ensure that customers are accepted only after carrying out appropriate due diligence in accordance with RBI Master Directions & applicable laws
- To prevent onboarding of customers whose identities or credentials are unverifiable, unreliable, or inconsistent with our KYC-AML framework.
- To align the Customer Acceptance Policy (CAP) with RBI guidelines and maintain a high-quality, compliant loan book by onboarding only verified customers.

2. Key Principles and Acceptance Norms

IITL shall ensure that:

1. **No Account in Anonymous or Fictitious Name:** Relationships shall not be initiated in fictitious, benami, or anonymous names.
2. **CDD as a Mandatory Prerequisite:** No account or transaction-based relationship shall be undertaken without completing Customer Due Diligence (CDD) in accordance with this Policy.
3. **Inability to Comply with CDD:** If CDD cannot be applied due to non-cooperation or unreliable documentation, the account shall not be opened. Such cases shall be evaluated for Suspicious Transaction Report (STR) filing with FIU-IND.
4. **Mandatory Information and Documentation:** Prescribed KYC documents and information must be submitted at onboarding and updated periodically. The list shall be in line with RBI and internal guidelines.
5. **Voluntary Additional Information:** Where additional data is sought (beyond prescribed norms), customer consent shall be explicitly obtained.
6. **Unique Customer Identification Code (UCIC):** A UCIC shall be assigned to each new and existing customer. CDD will be conducted at the UCIC level, covering borrowers, co-borrowers, guarantors, and beneficial owners.
7. **Reuse of Existing KYC Records:** If the customer has an active relationship with IITL and KYC details are up to date, duplication of CDD shall be avoided. However, updated due diligence may be carried out wherever necessary.
8. **Joint Relationships:** CDD shall be performed separately for each party involved in a joint loan facility or guarantee arrangement.
9. **Authorized Representatives / POA Holders:** Where a person is acting on behalf of another individual/entity, IITL shall record the authorisation and verify identity and intent.
10. **Sanctions Screening:** All customers shall be screened against relevant domestic and international sanctions lists (UN, FATF, RBI, etc.). Onboarding shall be denied for individuals/entities flagged on such lists.
11. **Verification of PAN and Other Registrations:** PAN shall be verified through the Income Tax database. GST numbers, if provided, shall be validated through GSTIN search tools.
12. **e-Documents and Digital Verification:** Where electronic documents are submitted, digital signatures and metadata shall be validated under the Information Technology Act, 2000.
13. **Onboarding High-Risk or Watch listed Customers:** Customers identified as high-risk or red-flagged by any regulator shall be subject to Enhanced Due Diligence (EDD) or may be declined onboarding.
14. **No Denial of Access to Financial Facilities:** CAP shall not be used to deny financial access to members of the general public, particularly those who are economically or socially disadvantaged. IITL shall balance financial inclusion and regulatory compliance.
15. **Avoiding Customer Tip-Off:** If suspicion of money laundering or terrorist financing arises, and completing CDD could alert the customer, IITL shall not proceed with CDD and will instead file an STR with FIU-IND.
16. **Central KYC (CKYC) Compliance:** IITL shall ensure compliance with the Central KYC (CKYC) norms as prescribed by the regulator. If a customer is being onboarded for the first time, IITL shall upload the KYC information to the Central KYC Registry maintained by CERSAI (Central Registry of Securitisation Asset Reconstruction and Security Interest of India). If a valid CKYC number already exists for an individual and the KYC information is up to date and verified, fresh KYC collection may be avoided. However, if there are any changes in the customer's details or any concerns or alerts

(such as mismatches or suspicious indicators), updated due diligence shall be carried out before onboarding. CKYC records shall be retrieved, verified, and stored as part of the KYC documentation process.

Risk Management

IITL adopts a risk-based approach (RBA) to customer due diligence in line with RBI's KYC Master Directions. This ensures appropriate levels of scrutiny are applied to customers based on perceived risks related to money laundering (ML), terrorist financing (TF), fraud, and regulatory exposure.

1. Risk Categorization Framework

Customers shall be categorized into Low, Medium, and High risk categories based on a combination of the following risk parameters:

- Identity Verification – nature and reliability of documents provided
- Geographical Risk – country, state, or locality of residence or business
- Nature of Business / Industry – vulnerability of sector to ML/TF
- Source of Funds / Occupation – transparency and traceability
- Delivery Channels – face-to-face vs. non-face-to-face interactions
- Transaction Type & Volume – cash vs. non-cash, domestic vs. international
- Regulatory or Sanctions Watchlists – UN, FATF, SEBI, RBI, etc.

2. Risk Categorization Table (Illustrative)

Category	Examples of Customers
Low Risk	Salaried employees (Govt or Pvt, bank salary), pensioners, individuals with verifiable income & stable profiles
Medium Risk	Salaried in cash, traders in high-risk areas, private limited companies, trusts, small businesses with inconsistent records
High Risk	Non-residents, PEPs, NGOs, bullion dealers, lawyers, high-cash volume professions, non-face-to-face customers, politically exposed, adverse media

Risk categorization shall be supported by a documented rationale and reviewed at least once every six months by the designated officer responsible for KYC compliance

Periodic Updation of KYC

Periodic updation of KYC records of existing customers to ensure that the customer identity, address, and other information remain relevant and up to date. The frequency of KYC updation shall be based on the customer's risk category, as under::

Risk Category	KYC Update Frequency
Low Risk	Every 10 years
Medium Risk	Every 8 years
High Risk	Every 2 years

4. Confidentiality of Risk Profile

The customer's risk category and the reason for classification shall be kept confidential to comply with anti-tipping-off norms and to maintain the integrity of monitoring.

5. Use of Global & Sectoral Guidance

In determining risk levels, IITL shall refer to the following:

- FATF Public Statements
- Indian Banks' Association (IBA) Guidance Notes
- Sector-specific alerts issued by RBI, FIU-IND, SEBI, etc.

These references shall inform risk classification practices and support compliance with domestic and global regulatory expectations.

6. Monitoring and Oversight

- The CEO -NBFC Operations shall oversee the risk categorization and ensure consistent application of this framework.
- Internal Audit and Compliance teams shall regularly review categorization adherence, with findings submitted to the Audit Committee.
- High-risk customers shall be subject to EDD, including more frequent reviews, additional documentation, physical verification (if required), and approval by senior authority.

CUSTOMER IDENTIFICATION PROCEDURE (CIP)

IITL shall undertake Customer Identification Procedure (CIP) to verify the identity of customers and ensure that relationships are established only with individuals or entities whose identity is clearly established through reliable and independent documents, data, or information. CIP is a mandatory part of Customer Due Diligence (CDD) and must be completed prior to establishing any financial relationship.

1. Applicability of CIP

IITL shall undertake Customer Identification Procedure in the following scenarios:

- At the time of establishing an account-based relationship with a customer.
- When there is any doubt regarding the adequacy of the customer's identification information, whether during onboarding or in the course of an ongoing relationship.

2. Prohibition on Introduction-Based Accounts

IITL shall not open any account solely based on the introduction by an existing customer or any third party. Introduction shall not be considered a substitute for carrying out the prescribed Customer Due Diligence (CDD) under applicable KYC norms.

3. Reliance on Third-Party Customer Due Diligence (CDD)

IITL may rely on CDD conducted by a third party, provided the following conditions are met:

- i. The third party is a Regulated Entity under RBI, SEBI, IRDAI and is supervised for compliance with KYC and record-keeping under the Prevention of Money Laundering Act, 2002.
- ii. The third party is not based in a high-risk jurisdiction as identified by the Financial Action Task Force (FATF) or competent Indian authorities.
- iii. CDD records or relevant customer information are obtained immediately from the third party or from the Central KYC Records Registry (CKYCR), as applicable.
- iv. The third party is capable of furnishing the customer's identification documents and relevant records upon request, without delay.
- v. The ultimate responsibility for conducting CDD, assigning risk category, and undertaking Enhanced Due Diligence (EDD), where applicable, shall remain with IITL.

CUSTOMER DUE DILIGENCE PROCEDURE

Customer Due Diligence (CDD)

Customer Due Diligence (CDD) means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

CDD process shall be applicable at the time of establishing an account-based relationship with a customer and shall also be undertaken while carrying out periodic updates.

Types of documents

Documents to be collected from the applicant/co-applicant /guarantor/any other party to the loan are as follows:

Entity-specific KYC Documents:

For Individuals, Proprietor / Partnership / HUF / Club / Trust / Societies or body of individuals / Limited Companies:

1. Application form with recent photograph of the applicant
 2. Proof of legal existence
 3. Proof of operating address
 4. Proof of registered address, if different from operating address
- Refer to Annexure II for the list of documents and manner of verification.

Annexure II

LIST OF DOCUMENTS TO BE OBTAINED AS AN INDIVIDUAL/ AS AN ENTITY AS A PROOF OF IDENTITY/ EXISTENCE AND PROOF OF ADDRESS

Type of Entity	Documents Required
Individual / Beneficial Owner / Authorised Signatory	1. Application Form with applicants photograph 2. Proof of Identity: a. PAN Card or Form 60 in the absence of PAN (Mandatory) b. Officially Valid Documents (OVDs): Passport, Voter ID,

	Driving License, Aadhaar or other prescribed document by RBI as per KYC Master Directions,2016 3. Proof of Address: a. Utility Bill (not older than 2 months) b. Property/Municipal Tax Receipt c. Bank Statement/Passbook or any other prescribed document by RBI as per KYC Master Directions,2016 d. Original Seen & Verified Stamp (OSV) by authorized employee with signature, date, ID
Proprietorship	1. Application Form with applicants photograph 2. Proof of Identity: PAN or Form 60 of Proprietor (Mandatory) 3. Proof of Business Activity (Any Two): a. Udyam Certificate b. Shop and Establishment License c. Sales/Income Tax Returns d. GST Certificate e. IEC Code f. Complete ITR (not just acknowledgement) g. Utility Bills (not older than 2 months)
Partnership Firm	1. Application Form 2. Registration Certificate of Firm 3. Partnership Deed 4. PAN of Firm 5. Identity & Address Proof of Authorized Signatories and Beneficial Owners 6. Beneficial Ownership Declaration (Annexure V) 7. Office Address Proof (Any One): a. Latest Telephone/Electricity/Water Bill or Tax Receipt
Company (Private/Public)	1. Application Form 2. Certificate of Incorporation 3. Memorandum & Articles of Association 4. PAN of Company 5. Board Resolution for Authorized Signatories 6. Identity & Address Proof of Authorized Signatories and Beneficial Owners 7. Beneficial Ownership Declaration (Annexure V) 8. Office Address Proof (Any One): a. Latest Telephone/Electricity/Water Bill or Tax Receipt
Trust / Society / Club	1. Application Form 2. Registration Certificate 3. Trust Deed 4. PAN or Form 60 5. Identity & Address Proof of Trustees and Authorized Signatories 6. Beneficial Ownership Declaration (Annexure V) 7. Office Address Proof (Any One): a. Latest Telephone/Electricity/Water Bill or Tax Receipt

Enhanced Due Diligence (EDD):

EDD in case of Non-Face-to-Face Customer Onboarding: Non-face-to-face onboarding includes use of digital channels such as CKYCR, Digi Locker, e-documents, and

1. V-CIP shall be provided as first option.
2. Alternate mobile numbers shall not be linked for transaction updates or OTPs.
3. Current address shall be verified through positive confirmation before disbursement.
4. PAN shall be mandatory and verified from issuing authority.
5. First payment must come from customer's KYC-complied account.
6. Customer shall be categorised as high-risk and subjected to enhanced monitoring till verification via face-to-face or V-CIP.

Accounts of Politically Exposed Persons (PEPs)

IITL may establish a lending relationship with PEPs or their relatives provided:

- Sufficient information on source of funds/wealth and identity is gathered.
- Identity is verified prior to relationship.
- Formal approval is taken from concerned official
- Enhanced monitoring is conducted ongoing.
- All PEP accounts are marked as High Risk.

Ongoing Due Diligence

IITL may undertake Ongoing Due Diligence (ODD) of its customers to ensure that their transactions and overall profile remain consistent with the information available at the time of onboarding or during periodic updates. The objective of ODD is to identify any material changes in customer risk, detect unusual activity, and update customer records in a timely and risk-based manner.

ODD may be carried out using the following measures:

1. Periodic re-verification of KYC documents and customer profile, as per prescribed timelines based on risk categorization
2. Review of loan repayment behaviour, including missed EMIs, delayed payments, cheque/ECS bounces, and restructuring requests, which may serve as early warning signals.
3. Collection and verification of updated documents such as financial statements, GST returns, ITRs, or bank statements
4. Conducting field verification or customer interaction (physical or digital) for high-value or high-risk clients, if required

Policy review & Update

This policy shall be reviewed periodically and placed before the Board of Directors for approval.

ANTI MONEY LAUNDERING POLICY

Anti-Money Laundering – Introduction

1.1. Money laundering refers to the process of making illegally-gained proceeds (i.e., “dirty money”) appear legal (i.e., “clean”). It typically involves disguising the origin of funds obtained through unlawful activities such as drug trafficking, terrorism, organized crime, corruption, fraud, or tax evasion. The objective of money laundering is to hide the true source and ownership of the funds and present them as coming from legitimate sources. This is achieved by introducing these illicit funds into the financial system through a complex web of transactions, thereby concealing their criminal origin and making them appear legally acquired.

1.2. Recognizing the global threat posed by money laundering, the United Nations adopted a political declaration and programme of action in 1990, urging member nations to enact national laws to combat this threat. In line with this global commitment, the **Government of India enacted the Prevention of Money Laundering Act, 2002 (PMLA)**, which came into effect on January 17, 2003. The Act forms the cornerstone of India's framework to detect and deter money laundering practices.

1.3. India’s expanding financial and credit ecosystem presents increased vulnerabilities to money laundering, particularly through non-banking channels. While traditional banking institutions remain a primary focus, NBFCs being in the business of providing loans and credit facilities—are also exposed to the risk of misuse for laundering illicit funds. Common sources of unlawful proceeds in India include narcotics trafficking, smuggling, corruption, tax evasion, and illegal trade. Such proceeds are often laundered through informal mechanisms like hawala, where funds are transferred across regions or countries without actual currency movement, obscuring the origin and audit trail. As a Non-Deposit Accepting Investment and Credit Company, IITL must remain vigilant to ensure its loan products and customer onboarding mechanisms are not exploited to introduce, layer, or integrate tainted funds. This makes robust implementation of KYC norms, Customer Due Diligence (CDD), and monitoring systems essential in safeguarding the institution from being unknowingly used for money laundering or terrorist financing.

Money Laundering Process

The process of money laundering typically involves **three distinct stages**, each designed to disguise the origin and trail of illicit funds:

1. Placement

This is the initial stage, where the proceeds of criminal activity are introduced into the financial system.

2. Layering

This stage involves a series of complex transactions intended to obscure the origin of the funds and make tracing difficult.

3. Integration

This is the final stage where the laundered money is re-introduced into the legitimate economy, appearing as clean and lawful income.

Appointment of Designated Director and Principal Officer

In accordance with the provisions of the Prevention of Money Laundering Act, 2002 (PMLA), the Rules made thereunder, and the RBI Master Direction on Know Your Customer (KYC), IITL has made the following appointments to ensure compliance with anti-money laundering obligations:

Designated Director

As per the applicable regulatory definition, the Designated Director is responsible for ensuring overall compliance with the obligations imposed under Chapter IV of the PMLA and the Rules framed thereunder. In the case of a company, the Designated Director shall be the Managing Director or a Whole-Time Director duly authorized by the Board of Directors.

Accordingly, the Board of IITL has appointed Whole Time Director, as the Designated Director. He shall be responsible for overseeing the implementation of the Anti-Money Laundering (AML) policy, ensuring adherence to regulatory requirements, and maintaining liaison with regulatory authorities, including FIU-IND and the Reserve Bank of India, in all AML/CFT matters.

Principal Officer

The Principal Officer, as defined under Rule 2(1)(f) of the PML Rules, is a senior management official nominated by the company who is responsible for the following:

- Implementation and monitoring of the day-to-day operations of the AML framework.
- Reporting of Cash Transaction Reports (CTR), Suspicious Transaction Reports (STR), and other prescribed reports to FIU-IND in accordance with Rule 8 of the PML Rules.
- Coordinating with law enforcement agencies, regulators, and other stakeholders as may be required under the law.

The Board of IITL has appointed *Chief Executive Officer (CEO)*, as the Principal Officer for this purpose.

Regulatory Intimation

Any changes in the appointment of the Designated Director or the Principal Officer shall be duly communicated to the Financial Intelligence Unit-India (FIU-IND), Reserve Bank of India (RBI), and other concerned authorities within the timelines prescribed under the applicable laws and regulations.

Maintenance and Preservation of Records of Transactions

In compliance with Section 12 of the Prevention of Money Laundering Act, 2002 (PMLA) and Rule 3 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, IITL shall ensure the proper maintenance and preservation of records of transactions, customer identification data, and related information in a secure and systematic manner.

1. Scope and Applicability

IITL shall maintain and preserve the following records and information for all loan customers and associated parties such as co-applicants, guarantors, and beneficial owners:

- Loan applications and related documentation.
- Records of all transactions, including sanctioned and disbursed loan amounts, repayments, interest payments, part-prepayments, foreclosure, and defaults.
- Any attempted transaction or suspicious activity related to a customer.
- KYC records including identification documents, address proofs, ownership declarations, CDD/EDD findings, and internal risk categorization.
- Communication and correspondence relating to business decisions and compliance.

2. Periodicity for Retention of Records

IITL shall follow the below guidelines for record retention:

Nature of Record	Minimum Retention Period
Records of all transactions (attempted or executed), including nature, amount, and parties involved	5 years from the date of transaction or account closure whichever is later
Customer identification documents, account files, beneficial ownership details, business correspondence, and internal analysis reports	5 years from the date of termination of the business relationship or account closure, whichever is later

3. Mode and Manner of Record Maintenance

- IITL shall maintain records in either physical or digital formats, ensuring integrity, confidentiality, and secure access.
- All such records shall be maintained in a manner that facilitates easy and quick retrieval for internal audits, compliance checks, or for furnishing to competent authorities, such as the Financial Intelligence Unit – India (FIU–IND), Enforcement Directorate, or RBI, upon request.

4. Access and Control

- Only authorized personnel shall be permitted access to transaction and identification records.
- Access logs and audit trails shall be maintained for every record retrieval or update.
- In the event of ongoing investigations or directions from regulators or law enforcement agencies, such records shall be preserved beyond the five-year period, if required.

5. Responsibility and Oversight

The Principal Officer shall ensure compliance with the above requirements and Periodic internal audits shall verify adherence to the retention policy and confirm the availability and completeness of records.

Monitoring of transactions and Reporting to Financial Intelligence Unit – India (FIU-IND)

1. Overview

In accordance with Section 12 of the Prevention of Money Laundering Act, 2002 (PMLA) and the PML Rules, IITL shall maintain a robust system of monitoring and reporting of specified financial transactions to the Financial Intelligence Unit – India (FIU-IND) through its designated Principal Officer.

The reporting framework includes:

- **Cash Transaction Reports (CTR)**
- **Suspicious Transaction Reports (STR)**

All reports shall be filed in electronic format only, as prescribed by FIU-IND, within the stipulated timelines. Confidentiality will be strictly maintained and no employee shall disclose to the customer about any such reporting.

2. Cash Transactions Reporting (CTR)

As a matter of policy, IITL does not accept any cash from customers for loan disbursement, repayment, or fees. All transactions are routed through regular banking channels such as NEFT, RTGS, IMPS, UPI, or Cheque/DD. Therefore, Cash Transaction Reporting (CTR) requirements under PMLA are not applicable.

3. Suspicious Transactions Reporting (STR)

IITL is a Non-Deposit accepting Non-Banking Financial Company (NBFC). It receives loan repayments through banking channels. IITL will file Suspicious Transaction Reports (STRs) with FIU-IND if any suspicious activity is noticed during loan processing or servicing.

Combating Financing of Terrorism (CFT)

IITL is committed to preventing the misuse of its financial services for terrorist financing. All customers, co-applicants, and guarantors are screened at onboarding and periodically thereafter against sanctioned lists issued under the UAPA, UNSCR, FATF, and other applicable sources. Any positive match is escalated to the Principal Officer and reported to FIU-IND and relevant authorities. No loan shall be processed or disbursed in such cases without proper clarification.

IITL ensures compliance with:

Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 by screening against notified terrorist entities and freezing accounts if required.

Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005), including daily screening against the designated list and immediate reporting of any match to the appropriate authorities and RBI

United Nations Security Council Resolutions Democratic People's Republic of Korea (DPRK) (UNSCR 1718 (DPRK) compliance through daily verification of MEA-published lists.

Money Laundering and Terrorist Financing Risk Assessment

IITL shall carry out a Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise in the month of May each year to identify, assess, and effectively mitigate the risks associated with clients, geographic locations, products, services, transactions, and delivery channels.

The risk assessment shall consider all relevant risk factors before determining the overall risk level and the appropriate level and type of mitigation required. While preparing this assessment, IITL shall consider sector-specific vulnerabilities shared by regulatory authorities, if any.

The risk assessment shall be appropriately documented and proportionate to IITL's nature, size, operational geography, and complexity of activities.

Secrecy Obligations and Sharing of Information

(a) IITL shall maintain strict confidentiality regarding customer information arising out of the contractual relationship between the Company and its customers.

(b) Information collected from customers for the purpose of loan sanctioning or onboarding shall be treated as confidential and shall not be used for cross-selling or any other purpose without the express consent of the customer.

(c) While considering requests for customer data or transaction information from government or other agencies, IITL shall ensure that the request does not violate the provisions of applicable laws relating to confidentiality and customer privacy.

(d) Exceptions to the above confidentiality obligation shall apply only under the following circumstances:

- i. Where disclosure is required under compulsion of law;
- ii. Where there is a public duty to disclose; and
- iii. Where disclosure is made with the express or implied consent of the customer.

Recruitment & Training

Recruitment

IITL shall establish and implement an adequate screening mechanism as an integral part of its recruitment and hiring process. This includes a Know Your Employee (KYE) or Staff Due

Diligence policy to ensure that individuals employed or associated with IITL are trustworthy, compliant, and do not pose any reputational or regulatory risk.

Training

All newly recruited employees, including members of the credit, operations, sales/advisory staff, Direct Selling Agents (DSAs), and field officers who interact with customers, shall be given general orientation on the risks and indicators of Money Laundering (ML) and Terrorist Financing (TF).

Additionally:

- Refresher training shall be conducted at regular intervals to keep staff updated on evolving KYC/AML/CFT regulatory requirements and internal responsibilities.
- The training content shall be role-specific:
 - Frontline and on-boarding staff shall be trained to identify unusual behaviour, improper documentation, and raise alerts.
 - Compliance and operations teams shall be trained in regulatory obligations, internal procedures, transaction monitoring, and reporting mechanisms (like STR/CTR).
 - Audit staff shall be staffed with individuals well-versed in AML/CFT regulations, risk-based approaches, and internal monitoring standards.