
Know Your Customer (KYC)
And
Prevention of Money
Laundering (PMLA) Policy

GLOSEC FINANCE PRIVATE LIMITED

Policy Statement

Glosec Finance Private Limited ("the Company") recognizes its role as a corporate entity and endeavors to adopt the best practices with the highest standards of governance through transparency in business ethics, accountability to its customers, government and others.

The Company has adopted the said KYC guidelines with suitable modifications depending on the activity undertaken by it. The Company has ensured that a proper policy framework on KYC and AML measures be formulated in line with the prescribed RBI guidelines and put in places duly approved by its Board of Directors.

The current version of the combined Policy on Know Your Customer (KYC) and Prevention of Money Laundering Activities (PMLA) is the updated version where a formal policy on PMLA has been integrated to the prevalent KYC Policy, duly edited in line with the latest guidelines of Reserve Bank of India.

The policy will be in compliance with the Reserve Bank of India (Non-Banking Financial Companies- Know Your Customer) Direction, 2025 vide notification number RBI/DOR/2025-26/361 Master Direction DOR.AML.REC.No.280/14.01.003/2025-26 and the guidelines mentioned therein, updated as an December 29, 2025, Anti-Money Laundering (AML), Combating of Financing of Terrorism (CFT) and obligations of regulated entities under Prevention of Money Laundering Act, (PMLA), 2002.

Objectives

In line with regulatory requirements and the nature of operations of the company, this KYC-AML-CFT Policy is designed to achieve the following objectives:

a) Prevention of Misuse

To prevent the Company from being used, intentionally or unintentionally, as a channel for money laundering or terrorist financing activities.

b) Customer Understanding (CDD)

To enable the Company to know and understand its customers, beneficial owners, and their financial dealings in order to manage risks effectively.

c) Risk-Based Approach (RBA)

To implement a risk-based framework for identification, classification, and monitoring of customers and transactions.

d) Detection and Reporting

To establish systems for timely identification and reporting of suspicious transactions to the appropriate authorities, including the Financial Intelligence Unit.

e) Regulatory Compliance

To ensure compliance with applicable laws, RBI directions, and internal policies.

f) Employee Awareness and Training

To ensure that all relevant staff are adequately trained on KYC, AML, and Counter Financing of Terrorism (CFT) requirements.

g) Proportionate Controls for NBFC-BL

Given the Company's classification as a Base Layer NBFC, to implement controls that are proportionate to the size, scale, and nature of operations, while fully complying with regulatory expectations.

Applicability & Scope

This Policy shall apply to all financial transactions and business relationships undertaken by the Company, including those with its customers, counterparties, and other stakeholders.

The Policy shall be applicable across the entire organization, including:

- The Board of Directors
- Senior Management
- Designated Director and Principal Officer
- All employees and staff members

The **Board of Directors** shall be responsible for:

- Approving the KYC-AML Policy
- Overseeing its effective implementation
- Ensuring periodic review in line with regulatory changes

The **Senior Management** shall ensure:

- Proper implementation of the Policy
- Allocation of responsibilities
- Establishment of internal controls and monitoring systems

All employees of the Company shall be responsible for **strict adherence** to the provisions of this Policy.

This Policy shall come into force with effect from the date of its approval by the Board of Directors and shall remain in force unless modified or replaced.

The Policy shall be applicable *to all branches, offices, and operational units of the Company* and shall be read in conjunction with:

- Internal operational guidelines
- Circulars and instructions issued from time to time
- Applicable laws and regulatory directions issued by the Reserve Bank of India

Core Elements of the Policy

In accordance with regulatory requirements, the Company's KYC Policy shall comprises of the following four key elements:

- (i) Customer Acceptance Policy;
- (ii) Risk Management;
- (iii) Customer Identification Procedures (CIP); and
- (iv) Monitoring of Transactions

The KYC policy also incorporate provisions for the following:

- (i) Periodic updation of KYC
- (ii) Any exceptional measures for KYC updation, such as requiring a recent photograph, physical presence, or a more frequent updation schedule than the minimum prescribed.
- (iii) Obtaining a copy of OVD or deemed OVD, for the purpose of proof of change of address during KYC updation.
- (iv) Providing facility of updation / periodic updation of KYC at any branch.
- (v) Change of registered Mobile Number for accounts opened in non-face-to-face mode.

Preventive Measures

The Company shall implement robust preventive measures to mitigate the risks of **Money Laundering (ML)** and **Terrorist Financing (TF)**, in line with the regulatory framework prescribed by the Reserve Bank of India.

The minimum standards shall include well-defined procedures for Customer Due Diligence (CDD), customer identification, verification, monitoring, and internal controls. All employees shall be responsible for identifying and promptly reporting any unusual or suspicious activity to the Principal Officer.

a)	Customer Acceptance Policy (CAP)	<p>The Company shall establish a Customer Acceptance Policy as part of its internal operational guidelines, which shall:</p> <ul style="list-style-type: none">• Clearly define criteria for acceptance of customers based on risk categorisation (Low/Medium/High)• Prohibit opening of accounts in anonymous or fictitious/benami names• Ensure that no customer is onboarded without completion of Customer Due Diligence (CDD)• Provide for Enhanced Due Diligence (EDD) in case of high-risk customers
----	----------------------------------	--

		<ul style="list-style-type: none"> • Include sanctions screening (UN and domestic lists) prior to onboarding.
b)	Customer Identification Procedure (CIP)	<p>The Company shall carry out Customer Identification Procedure:</p> <ul style="list-style-type: none"> • At the time of establishing a business relationship • While undertaking transactions as prescribed under RBI guidelines <p>CIP shall include:</p> <ul style="list-style-type: none"> • Collection and verification of Officially Valid Documents (OVDs) • Aadhaar (voluntary), PAN/Form 60, and other prescribed documents • Identification of Beneficial Owner (BO) in case of non-individual customers • Use of Digital KYC / Video Customer Identification Process (V-CIP), wherever applicable
c)	Customer Due Diligence (CDD) and Verification	<p>The Company shall:</p> <ul style="list-style-type: none"> • Obtain recent photograph and KYC details of customers • Verify identity and address through reliable and independent sources • Conduct field verification (residence/business) where considered necessary based on risk assessment • Understand the purpose of the relationship and source of funds
d)	Risk-Based Approach (RBA)	<p>The Company shall adopt a risk-based approach by:</p> <ul style="list-style-type: none"> • Classifying customers into Low, Medium, and High Risk categories • Applying proportionate due diligence measures • Conducting periodic review of risk categorisation • Applying Enhanced Due Diligence (EDD) for high-risk categories such as PEPs, non-residents, and complex structures
e)	Credit and Background Checks	<p>Prior to granting any credit facility, the Company shall:</p>

		<ul style="list-style-type: none"> • Conduct credit bureau checks through authorised Credit Information Companies (CICs) • Assess creditworthiness and repayment capacity • Perform reference checks, where applicable, and maintain proper documentation
f)	Record Management and MIS	<p>The Company shall:</p> <ul style="list-style-type: none"> • Maintain complete and updated customer records in its Management Information System (MIS) • Ensure that KYC and transaction records are preserved for at least 5 years as per regulatory requirements • Maintain proper audit trail of all transactions and customer interactions
g)	Ongoing Monitoring and Transaction Surveillance	<p>The Company shall:</p> <ul style="list-style-type: none"> • Continuously monitor transactions to ensure consistency with customer profile and risk categorisation • Identify: <ul style="list-style-type: none"> ○ Unusual patterns ○ Large or complex transactions ○ Transactions lacking economic rationale <p>The IT systems shall be enabled to:</p> <ul style="list-style-type: none"> • Generate alerts for suspicious transactions • Facilitate timely reporting to the Principal Officer
h)	Employee Due Diligence and Training	<p>The Company shall:</p> <ul style="list-style-type: none"> • Implement proper employee screening procedures at the time of recruitment • Obtain and verify KYC details of employees • Provide periodic training programs on KYC/AML/CFT to: <ul style="list-style-type: none"> ○ Frontline staff ○ Operations team ○ Compliance personnel <p>Training shall be aligned with job roles and updated regulatory requirements.</p>
i)	Internal Controls and Audit	<p>The Company shall:</p>

		<ul style="list-style-type: none"> • Establish a robust internal control framework • Ensure independent audit of KYC/AML processes • Deploy adequately trained personnel for audit and compliance functions • Report findings to the Board/Audit Committee
j)	Technology and Systems	<p>The Company shall implement appropriate IT systems to:</p> <ul style="list-style-type: none"> • Support KYC compliance and record keeping • Enable risk-based transaction monitoring • Generate automated alerts for suspicious activities • Maintain secure and tamper-proof data
k)	Due Diligence in Fund Raising	<p>While raising funds from entities other than:</p> <ul style="list-style-type: none"> • Banks, or • Regulated Financial Institutions <p>The Company shall:</p> <ul style="list-style-type: none"> • Conduct adequate due diligence on counterparties • Assess legitimacy and source of funds • Report any suspicious activity to the Principal Officer
l)	Responsibility of Management and Board	<p>The Board of Directors and Senior Management shall ensure that:</p> <ul style="list-style-type: none"> • These preventive measures are effectively implemented • All product and operational policies incorporate KYC/AML requirements • Adequate systems, controls, and resources are in place for compliance
<p>*Specific responsibilities and actions of the Board and Senior Management for the above measures are elaborated in Reserve Bank of India (Non-Banking Financial Companies- Know Your Customer) Direction, 2025 vide notification number RBI/DOR/2025-26/361 Master Direction DOR.AML.REC.No.280/14.01.003/2025-26 and the guidelines mentioned therein, updated on December 29, 2025.</p>		

Guidelines on Prevention of Money Laundering (PMLA), 2002

The Prevention of Money-Laundering Act, 2002, and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT). The provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, require Regulated Entities (REs) to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise, and to monitor their transactions. The general guidelines are as follows:

1. Appointment of Key Officials

- The Company shall appoint:
 - a **Principal Officer** responsible for monitoring transactions and reporting to FIU-IND; and
 - a **Designated Director** to ensure overall compliance with PMLA obligations.
- The details of such officials shall be communicated to RBI and FIU-IND.

2. Internal Reporting Mechanism

- The Company shall establish a robust **internal reporting system** to identify and report:
 - Suspicious Transactions
 - Cash Transactions and structured transactions
- All employees shall be trained to escalate suspicious activities to the Principal Officer.

3. Maintenance of Records (As per PML Rules, 2005)

The Company shall maintain records of the following transactions:

(i) Cash Transactions

- All cash transactions exceeding ₹10 lakh or its equivalent in foreign currency

(ii) Series of Cash Transactions

- Integrally connected cash transactions below ₹10 lakh, where aggregate exceeds ₹10 lakh in a month

(iii) Fraudulent Transactions

- Transactions involving forged or counterfeit currency or forged securities

(iv) Suspicious Transactions

- All suspicious transactions, whether cash or non-cash, including attempted transactions

4. Information to be Maintained

The Company shall maintain sufficient details to reconstruct individual transactions, including:

- Nature of transaction
- Amount and currency
- Date of transaction
- Parties involved in the transaction

5. Preservation of Records

The Company shall ensure proper maintenance and preservation of records as follows:

- (i) Maintain all transaction records (domestic and international) for a minimum period of five (5) years from the date of the transaction.
- (ii) Such records shall be sufficient to reconstruct individual transactions so as to provide evidence for investigation and prosecution, wherever required
- (iii) Records shall include details of:
 - Amount and type of currency
 - Date and nature of transaction
 - Parties to the transaction
- (vi) The records shall be maintained in hard copy or electronic form and shall be readily retrievable for submission to regulatory or enforcement authorities upon request.

Board Approval, Review and Disclosure

(i) Board Approval

- The policy shall be approved by the Board of Directors of the Company.

(ii) Periodic Review

- The policy shall be reviewed annually or whenever there are changes in regulatory guidelines issued by the Reserve Bank of India.
- Any amendments to the Code shall be approved by the Board of Directors.

(iii) Publication and Display

- The Company shall publish the KYC policy on its website, if available.
- A copy of the Policy shall be displayed at the registered office and other business locations of the Company for the information of customers.
- The Policy shall be made available to customers upon request.

