Document Title: Policy Guidelines on 'Know Your Customer'(KYC) norms and Anti-Money Laundering (AML) measures	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

Reliance Capital Limited

Policy Guidelines on 'Know Your Customer'(KYC) norms and Anti-Money Laundering (AML) measures

This document is copyright protected in content, presentation, and intellectual origin, except where noted otherwise. You may not modify, remove, augment, add to, publish, transmit, participate in the transfer or sale of, create derivative works from, or in any way exploit any of the elements of this document, in whole or in part without prior written permission from Reliance Capital Ltd. © 2025-2026.

Document Title: Policy Guidelines on 'Know Your Customer'(KYC) norms and Anti-Money Laundering (AML) measures	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

Table of Contents

1. Introduction
2. Objective
3. Definitions
4. Customer Acceptance Policy (CAP)
    - 4.1 General Principles
    - 4.2 Risk Categorization of Customers
    - 4.3 Customer Identification Procedure (CIP)
        - 4.3.1 Documents for Customer Identification
        - 4.3.2 Procedure for Digital KYC
    - 4.4 Beneficial Ownership Identification
5. Customer Due Diligence (CDD)
    - 5.1 General CDD
    - 5.2 Enhanced CDD (EDD)
    - 5.3 Simplified CDD
    - 5.4 Ongoing Due Diligence
    - 5.5 Politically Exposed Persons (PEPs)
6. Risk Management
    - 6.1 Risk Assessment
    - 6.2 Risk Mitigation
7. Monitoring of Transactions
    - 7.1 Transaction Monitoring
    - 7.2 Suspicious Transaction Reporting (STR)

8. Record Keeping
    - 8.1 Maintenance of Records
    - 8.2 Retention of Records
9. Reporting Requirements
    - 9.1 Reporting to Financial Intelligence Unit - India (FIU-IND)
    - 9.2 Other Reporting Obligations
10. Compliance with International Agreements
11. Employee Training
12. Technology Solutions for KYC/AML Compliance
13. Internal Audit
14. Policy Review
15. Amendments to the Policy

Document Title: Policy Guidelines on 'Know Your Customer'(KYC) norms and Anti-Money Laundering (AML) measures	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

1. Introduction:

Reliance Capital Limited NBFC CIC ("Company") is committed to strictly follow and comply the Reserve Bank of India (RBI) has issued guidelines on 'Know Your Customer' (KYC) Guidelines - Anti Money Laundering Standards for Non- Banking Financial Companies (NBFCs) thereby setting standards for prevention of money laundering activities and corporate practices while dealing with their customers vide various Circulars from time to time.

RBI has issued Master Direction – Know Your Customers (KYC) Directions, 2016 vide Master Direction No. DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016 which was last updated on November 6, 2024. These directions have been issued under sections 45L and 56 of the Chapter IIIB of the Reserve Bank of India Act, 1934, read with section 11(1) of the Banking Regulation Act, 1949, and rule 9 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. These directions shall apply to every Non-Banking Financial Company (NBFC) as defined in paragraph 2 of the Master Direction.

The Company is committed to be fully compliant with the KYC/AML norms and guidelines issued by the Reserve Bank of India. To achieve this objective, the Company has framed a comprehensive policy framework, incorporating the KYC and AML guidelines.

2. Objective:

The objective of these KYC/AML guidelines is to prevent Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. These guidelines also mandate that the Company have a proper policy framework in place, with Board approval, and ensure they are aware of their customers, their financial transactions, and the potential risks associated with them.

3. Definitions:

- "Anti-Money Laundering" (AML) refers to the laws, regulations, and procedures aimed at preventing the concealment of illicitly obtained funds.
- "Customer" means a person or entity that maintains an account and/or has a business relationship with the NBFC.
- "Know Your Customer" (KYC) refers to the process of identifying and verifying the identity of customers.
- "NBFC" means a Non-Banking Financial Company as defined in the RBI Master Direction.
- Other relevant definitions as per RBI Master Direction.
- "Designated Director" means a person from the senior management, who shall be notified to the Financial Intelligence Unit – India (FIU-IND)
- "Financial Institution" includes the following
  - A bank, public financial institution, as defined in section 2(72) of the Companies Act, 2013
  - The Reserve Bank of India
  - A subsidiary of a banking company
  - A co-operative bank
  - A housing finance institution
  - An insurance company
  - A mutual fund company
  - A pension fund company
  - A stock broker, sub-broker, share transfer agent, banker to an issue, trustee to trust deed, registrar to issue, merchant banker, underwriter,

portfolio manager, investment advisor or any other intermediary associated with the securities market and registered with the Securities and Exchange Board of India

- A chit, money-lender, pawnbroker, benefit fund company, nidhi company, society, trust, co-operative society or unincorporated body
- A company carrying on the business of chit fund or a company which receives monies under any scheme or arrangement or in any other manner but does not include a company which is a non-banking financial company
- A payment system provider or a payment system participant
- Such other institution as may be notified by the Central Government

- "Suspicious transaction" means a transaction whether or not relating to cash which, to a person acting in good faith –
  - Gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence, or
  - Appears to be made in circumstances of unusual or unjustified complexity, or
  - Appears to have no economic rationale or justification.
- "Beneficial Owner" means the natural person(s) who ultimately owns or controls a customer, including a legal person.
- "Shell bank" means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.
- "Wire transfer" means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a

bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.

- "Domestic and cross-border wire transfer": When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.
- All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

4. Customer Acceptance Policy (CAP):

This policy establishes the criteria for customer acceptance, ensuring that the Company does not unintentionally facilitate money laundering or other illegal activities.

4.1 General Principles

The CAP shall clearly define the types of customers that pose a higher risk and outline the enhanced due diligence measures that will be applied to them.

The CAP shall be applied consistently to all customers without any discrimination.

The CAP shall include guidelines for customer identification, risk assessment, and ongoing monitoring.

Ensure that the identity of the customer does not match with any person with known criminal background or with banned entities.

The Company should not have any relationship with shell bank.

4.2 Risk Categorization of Customers

The Company shall categorize customers into risk categories (e.g., low, medium, high) based on factors such as:

Customer's background, nature of business activity, location, country of origin, sources of funds, customer profile etc.

Volume of turnover, source of wealth, paying capacity

Clarity of purpose of the transaction

History of violations

Higher risk customers shall be subject to enhanced due diligence measures.

4.3 Customer Identification Procedure (CIP)

The CIP shall specify the documents required to verify the customer's identity.

The Company shall verify the identity of each customer and confirm that the information provided is correct.

The Company shall establish procedures for verifying the authenticity of documents provided by the customer.

The Company may use reliable electronic means for customer identification, subject to RBI regulations.

4.3.1 Documents for Customer Identification

For individuals, acceptable documents may include:

Passport

PAN Card

Aadhaar Card

Voter's Identity Card

Driving License

Identity card issued by the Central/State Government or Scheduled Commercial Banks or Public Sector Undertakings.

Utility Bill

Bank statement

Proof of address

For legal entities, acceptable documents may include:

Certificate of incorporation

Memorandum and articles of association

PAN Card

Board resolution for conducting business

GST Certificate

List of directors and their identification documents

4.3.2 Procedure for Digital KYC

The Company may undertake the Digital KYC process as per the RBI guidelines.

4.4 Beneficial Ownership Identification

The Company shall identify the natural person(s) who ultimately own or control the customer.

If the customer is a legal entity, the Company shall identify the beneficial owner(s) of that entity.

The Company shall take reasonable measures to verify the identity of the beneficial owner(s).

5. Customer Due Diligence (CDD):

This involves the degree of scrutiny and investigation undertaken to verify the customer's identity and assess the potential risks associated with the business relationship.

5.1 General CDD

Verify the customer's identity using reliable and independent source documents, data or information

Identify the beneficial owner, if any and take reasonable measures to verify the identity of the beneficial owner

Understand the nature of the customer's business

Conduct ongoing due diligence of the business relationship

5.2 Enhanced CDD (EDD)

The Company shall perform enhanced due diligence for customers identified as high-risk.

EDD measures may include:

Obtaining additional information about the customer and their business

Conducting on-site visits

Verifying the source of funds

Obtaining senior management approval for establishing or continuing the business relationship

Increased monitoring of the business relationship

5.3 Simplified CDD

The Company may apply simplified due diligence measures for customers identified as low-risk.

Simplified measures may include:

Collecting only the basic customer identification data

Lower frequency of monitoring

5.4 Ongoing Due Diligence

The Company shall conduct ongoing due diligence of the customer relationship to ensure that transactions are consistent with the customer's profile and risk category.

The frequency and extent of ongoing due diligence shall be determined by the customer's risk category.

5.5 Politically Exposed Persons (PEPs)

The Company shall establish procedures for identifying and dealing with Politically Exposed Persons (PEPs).

PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country.

The Company shall apply enhanced due diligence measures for PEPs, including:

Obtaining senior management approval before establishing a business relationship with a PEP

Taking reasonable measures to establish the source of funds and source of wealth of the PEP

Conducting enhanced ongoing monitoring of the business relationship

6. Risk Management:

The Company shall have a risk management system for KYC/AML compliance.

6.1 Risk Assessment

The Company shall conduct a risk assessment to identify and evaluate the money laundering and terrorist financing risks.

The risk assessment shall consider various factors, including customer demographics, geographic location, products and services offered, and transaction volumes.

6.2 Risk Mitigation

The Company shall implement appropriate risk mitigation measures to manage and reduce the identified risks.

Risk mitigation measures may include:

Enhanced customer due diligence

Transaction monitoring

Limitations on certain types of transactions

Employee training

7. Monitoring of Transactions:

The Company shall monitor customer transactions to identify any suspicious or unusual patterns.

7.1 Transaction Monitoring

* The Company shall implement a system for monitoring customer transactions.

* The monitoring system shall be capable of detecting various types of suspicious transactions, including:

* Large or unusual transactions

* Transactions with no apparent economic purpose

* Transactions involving high-risk countries

* The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

* The Company will examine the background and purpose of all such transactions, and also examine the possible link, if any, between such transactions with criminal activities including financing of terrorism.

7.2 Suspicious Transaction Reporting (STR)

* The Company shall report suspicious transactions to the Financial Intelligence Unit - India (FIU-IND) in the prescribed format and within the specified timeframe.

* The Company shall ensure that employees are aware of the procedure for reporting suspicious transactions.

* The fact of furnishing of suspicious transactions to FIU-IND shall be treated as confidential and shall not be disclosed to the customer.

8. Record Keeping:

The Company shall maintain proper records of customer identification and transactions.

8.1 Maintenance of Records

* The Company shall maintain all necessary records of customer identification and transaction data.

* These records shall be maintained in a manner that allows for easy retrieval.

* The Company shall ensure the confidentiality and security of these records.

8.2 Retention of Records

* The Company shall retain records for the period specified by the RBI and other applicable laws.

* Typically, records related to customer identification should be retained for at least five years after the business relationship has ended. Transaction records should also be retained for at least five years.

9. Reporting Requirements:

The Company shall comply with all reporting requirements as mandated by the regulatory authorities.

9.1 Reporting to Financial Intelligence Unit - India (FIU-IND)

* The Company shall report suspicious transactions to FIU-IND as per the prescribed guidelines.

* The reports shall be submitted in the prescribed format and within the specified timeframe.

9.2 Other Reporting Obligations

* The Company shall comply with any other reporting requirements as specified by the RBI or other regulatory authorities.

10. Compliance with International Agreements

The Company shall adhere to the obligations under international agreements, such as the Prevention of Money-Laundering (PML) Act and any other applicable laws and regulations.

11. Employee Training

The Company shall provide regular training to its staff on KYC/AML policies and procedures.

* Training shall cover customer identification, due diligence, transaction monitoring, and reporting requirements.

* Maintain records of employee training.

12. Technology Solutions for KYC/AML Compliance

The Company shall implement appropriate technology solutions for KYC/AML compliance, including:

* Customer screening software

* Transaction monitoring systems

* Electronic record management systems

* Ensure that the technology solutions are updated regularly to address emerging risks.

13. Internal Audit

The Company shall conduct periodic internal audits to assess the effectiveness of the KYC/AML framework.

* The internal audit shall cover all aspects of the KYC/AML policy and procedures.

* Findings of the internal audit shall be reported to senior management and the Board.

14. Policy Review

This policy shall be reviewed and updated at least once a year to ensure compliance with the latest regulatory requirements and best practices.

* The review shall be approved by the Board of Directors.

15. Amendments to the Policy

Any amendments to this policy shall be approved by the Board of Directors.

* The Company shall communicate any changes to the policy to all relevant staff members.