# THE MAHAVEER CO-OP. BANK LTD., BELAGAVI

## KYC & AML POLICY

**POLICIES FOR THE FY**
2026-27
https://mahaveerbank.bank.in

**Approved by the Board of Directors at its meeting held on 23/6/2026, vide Resolution No. 11 .**

## Introduction

This Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy is prepared as per the Prevention of Money Laundering Act (PMLA), 2002, related rules, and RBI KYC guidelines, as updated from time to time.

Banks can sometimes be misused for illegal activities like money laundering, fraud, terrorist financing, and identity theft. Therefore, it is important to have a strong KYC and AML system to prevent such misuse and to follow all legal and regulatory requirements.

This policy provides clear guidelines for identifying customers, verifying their details, monitoring transactions, and reporting suspicious activities. It also shows the Bank's commitment to transparency, safety, and preventing misuse of banking services under any circumstances.

## Objectives of the Policy

The primary objectives of this KYC & AML Policy are:

- To identify and verify the identity of all customers clearly
- To prevent the Bank from being used for illegal activities like money laundering, fraud, and terrorist financing
- To classify customers based on risk and apply proper checks
- To monitor customer transactions on a regular basis
- To detect and report suspicious transactions to the concerned authorities
- To follow RBI guidelines and legal requirements under PMLA
- To maintain proper and updated records of customers and transactions
- To ensure transparency and build trust in banking operations
- To improve staff awareness and ensure proper implementation of the policy
- To protect the Bank from financial and reputational risks

## Overview

This policy covers three key areas: KYC (Know Your Customer), AML (Anti-Money Laundering), and CFT (Combating Financing of Terrorism). Together, these help the Bank carry out its operations in a safe, secure, and lawful manner.

**KYC (Know Your Customer)** means the Bank must properly identify and verify every customer before opening an account. It also helps the Bank understand the customer's background, source of funds, and expected transactions. This reduces the risk of fraud and misuse of accounts.

**AML (Anti-Money Laundering)** refers to the steps taken by the Bank to prevent illegal money from entering or moving through the banking system. The Bank monitors customer transactions regularly to identify unusual patterns and reports suspicious activities to the authorities.

**CFT (Combating Financing of Terrorism)** means ensuring that the Bank's services are not used to support terrorist activities or organizations. The Bank checks customers against government and international sanction lists and closely monitors high-risk transactions.

This KYC, AML & CFT Policy is framed for the purpose of establishing a uniform and effective framework within the Bank to ensure regulatory compliance and sound banking practices. The policy is applicable to:

- All branches, departments, and administrative offices of the Bank.
- All existing and new customers, including individuals, proprietorships, partnerships, companies, trusts, societies, and other legal entities.
- All types of accounts, including savings accounts, current accounts, term deposits, loan accounts, and other banking relationships.
- All employees of the Bank involved in customer on boarding, servicing, and transaction processing.
- All outsourced agencies, agents, and service providers engaged in customer verification or related banking activities

## Applicability

This Policy shall be applicable to The Mahaveer Co-operative Bank Ltd., Belagavi and shall cover:

**Institutional Coverage**

- All branches, extension counters, and administrative offices of the Bank
- All departments, including operations, credit, deposits, treasury, and IT

**Personnel Coverage**

- All employees, including permanent, temporary, contractual, and outsourced staff
- Directors, officers, and management personnel responsible for customer onboarding and transaction monitoring

**Customer Coverage**

This Policy applies to all categories of customers, including:

- Individuals (resident and non-resident)
- Proprietorship concerns
- Partnership firms
- Companies and corporate entities
- Trusts, NGOs, and charitable institutions
- Government and semi-government bodies
- Nominal and associate members

**Product & Service Coverage**

The Policy shall apply to all products and services offered by the Bank, including:

- Savings, Current, Fixed Deposit, and Recurring Deposit accounts
- Loan and advance accounts (all categories)
- Remittance services (NEFT/RTGS/IMPS/DD)
- Locker facilities
- ATM/Debit card services
- Internet and mobile banking
- Third-party products, if any

**Transaction Coverage**

- All domestic and cross-border transactions
- Cash and non-cash transactions
- One-time transactions (walk-in customers)
- High-value and suspicious transactions

## DEFINITIONS

In this policy, the following terms shall have the meanings given below. These definitions are as per the Prevention of Money Laundering Act, 2002 (PMLA) and related Rules, as amended from time to time.

### 1.1 Terms defined under PMLA, 2002 and PML Rules, 2005

**1. Aadhaar Number**

"Aadhaar number" means a 12-digit unique identification number issued by the Unique Identification Authority of India (UIDAI) to an individual. It is based on the person's demographic and biometric details under the Aadhaar Act, 2016.

**2. Act and Rules**

"Act" means the Prevention of Money Laundering Act, 2002, which is made to prevent money laundering and to take action against illegal money.
"Rules" means the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, which explain how to maintain records, verify customers, and report transactions.
These are updated from time to time, and the Bank will follow all such updates.

**3. Authentication**

"Authentication" means the process of verifying a person's identity by using Aadhaar number along with demographic or biometric details.
This information is sent to the Central Identities Data Repository (CIDR) for checking.
If the details match, confirmation is received electronically.
This helps in safe and reliable customer verification and reduces identity fraud.

**4. Beneficial Owner (BO)**

Beneficial Owner means the actual person who finally owns or controls a customer or account, as given below:

(a) Company:
A person who:

- owns more than 25% of shares, capital, or profits, or
- has control over company decisions (like appointing directors or influencing management)

(b) Partnership Firm:
A person who owns more than 15% of capital or profits

(c) Unincorporated Association / Body of Individuals:
A person who owns more than 15% of property, capital, or profits

(d) Trust:
Includes:

- the author (creator) of the trust
- the trustee(s)
- beneficiaries with 15% or more interest
- any person who has final control over the trust

**5. Central Identities Data Repository (CIDR)**

CIDR is a central database maintained by UIDAI.
It stores Aadhaar numbers along with personal and biometric details.

It is used for identity verification and authentication.
Banks use it for e-KYC and secure customer verification.

**6. Central KYC Records Registry (CKYCR)**
CKYCR is a central system where customer KYC details are stored in digital form.
Once KYC is done, customers do not need to submit documents again to other banks.
Banks upload and update KYC details in this system.
It makes the process simple, faster, and more efficient.

**7. Demographic Information**
Demographic information means basic personal details like name, date of birth, gender, and address.
It is used for identity verification and KYC process.
It does not include sensitive details like religion, caste, income, or medical history.
It is used only for banking and legal purposes.

**8. Designated Director**
A Designated Director is a senior official of the Bank responsible for ensuring compliance with PMLA rules.
He/She oversees the AML and KYC systems of the Bank.
The Director ensures proper implementation of policies and reporting.
He/She also coordinates with regulators and authorities.

**9. Enrolment Number**
Enrolment Number is a 28-digit temporary number given at the time of Aadhaar application.
It is used to track the status of Aadhaar generation.
It is not a permanent number but only for temporary use.

**10. E-KYC Authentication Facility**
E-KYC is a digital method of customer verification using Aadhaar.
It uses OTP or biometric for identity confirmation.
After verification, UIDAI shares KYC details securely.
It reduces paperwork and speeds up account opening.

**11. Identity Information**
Identity information includes Aadhaar number, biometric data, and personal details of a customer.
It is used to verify identity during banking transactions.
This helps in preventing fraud and misuse of accounts.

**12. Non-Profit Organization (NPO)**
NPOs are entities like Trusts, Societies, and Section 8 Companies working for social or charitable purposes.
They do not operate for profit.
Banks must carefully verify their details as they are considered higher risk.

Registered as:
- Trust
- Society
- Section 8 Company

**13. Officially Valid Document (OVD)**
OVD means documents accepted for identity and address proof.
These include:

- Passport
- Driving Licence
- Voter ID
- NREGA Job Card
- NPR Letter

These documents are used for KYC verification.

**14. Person**
"Person" includes:
- Individual
- Hindu Undivided Family (HUF)
- Company
- Partnership Firm
- Association or group of persons
- Any legal entity or organization
- Any branch or office of such entities

**15. Principal Officer**
Principal Officer is a senior bank officer responsible for AML compliance.
He/She reports suspicious transactions to FIU-IND.
The officer ensures proper implementation of AML policies.
He/She acts as a link between the Bank and regulators.

**16. Resident**

A Resident is a person who is considered to be ordinarily residing in India based on the duration of stay in the country during the relevant period.

A person is treated as a Resident if they have stayed in India for 182 days or more in the 12 months immediately preceding the date of application or assessment.

This classification is used for Aadhaar eligibility and related identification and compliance purposes under applicable regulations.

**17. Suspicious Transaction**

A transaction, including an attempted transaction, which gives rise to reasonable grounds of suspicion that it may involve, directly or indirectly, the proceeds of crime or terrorist financing, and/or that it:

- involves funds derived from illegal or unauthorized activities, or
- has no apparent economic, lawful, or legitimate purpose, or
- is inconsistent with the customer's known profile, business activity, income pattern, or transaction history, or
- appears unusually complex, structured, or repetitive without reasonable justification, or
- is designed to evade reporting requirements or regulatory scrutiny, or
- may be linked, directly or indirectly, to money laundering, fraud, or terrorist financing activities.

**18. Small Account**

A Small Account is a simplified bank account opened for individuals who are unable to provide standard KYC documents, subject to prescribed regulatory limits.

The account is subject to the following restrictions:

- The total credits in a financial year shall not exceed ₹1,00,000.
- The maximum balance at any point of time shall not exceed ₹50,000.
- The total debits/withdrawals in a month shall not exceed ₹10,000.

Government benefits are not counted in balance limits.

**19. Transaction**

A Transaction includes any activity or arrangement involving a customer and the bank, whether conducted in cash, cheque, electronic form, or any other mode.

It includes, but is not limited to:

- Opening, operating, or closing of an account
- Deposits, withdrawals, transfers, or remittances
- Sanction, disbursement, repayment, or settlement of loans or advances
- Purchase or sale of financial instruments or services
- Use of safe deposit lockers or related facilities
- Any other financial activity, service, or contractual arrangement with the bank that results in movement of funds or change in account status

## Customer Acceptance Policy (CAP)

- Bank will do customer identification as the first and compulsory step before opening any account or starting any financial relationship.
- Identification will be done strictly as per RBI KYC rules and PMLA guidelines.
- Bank will collect and verify basic details like full name, photo, date of birth, address, nationality and contact details.
- Identity will be verified using valid documents (OVD) such as:
  - o Aadhaar
  - o PAN Card
  - o Passport
  - o Voter ID
  - o Driving License
  - o etc., as allowed under rules.
- Bank will take PAN card or Form 60 from all customers as per Income Tax rules.
- For non-individual customers, Bank will verify documents like Incorporation Certificate, Partnership Deed, Trust Deed, Bye-laws or Registration Certificate.
- Bank will identify and verify all authorized signatories and take proper permission (mandate) for account operation.
- Bank will identify the real owner (Beneficial Owner / UBO) and verify ownership and control details of all entities.
- Customer identification will be done through physical verification, Video KYC (V-CIP), digital KYC or other RBI approved methods.
- Bank will ensure all documents are genuine, valid, updated and not tampered.

- If any mismatch, doubt or suspicious information is found, it will be checked and cleared before account opening.
- Bank will check sanction list and negative list during identification process.
- Bank will not open account if customer identity is incomplete or doubtful.
- Bank will keep proper records of all KYC documents and verification for audit and inspection.
- No account will be opened unless full CIP is completed and approved by concerned authority.

## CKYC (Central KYC Registry)

- CKYC means Central KYC Registry, maintained by CERSAI.
- It is a single place where customer KYC records are stored and shared with all banks and financial institutions.
- After CKYC registration, customer gets a unique KYC ID.
- This KYC ID can be used to open account in any bank without doing full KYC again.
- CKYC helps to avoid repeated KYC and makes account opening easy and fast.
- Bank will upload, update and download KYC data in CKYC system as per RBI rules.
- CKYC ensures standard process, transparency and better monitoring of customers.
- It also helps in audit, inspection and easy verification of customer details.

## Guidelines on Introduction of Customer

- Introduction of customer is an additional support process to help verify the identity of a new customer, wherever required as per internal rules.
- Introduction should be taken from an existing customer of the Bank or a known person with good background, who has completed proper KYC.
- The introducer must have a satisfactory and regular banking relationship with the Bank for a reasonable period.
- The introducer should personally know the customer and confirm his/her identity and address.
- Introduction will not replace compulsory KYC documents like OVD and proper verification.
- Bank will use introduction only as a supporting reference, not as main identity proof.
- Branch staff should be careful and ensure that the introducer is genuine, traceable and not involved in any suspicious activity.

- Details of introducer should be properly recorded in account opening form and maintained for audit and verification.
- In all cases, RBI KYC rules and PMLA guidelines must be followed, even if introduction is given.
- Introduction will not be accepted for high-risk customers or cases requiring enhanced due diligence (EDD).

## Customer Due Diligence (CDD)

- Customer Due Diligence means checking and understanding the customer properly before opening account.
  Bank should know who the customer is and why they are opening the account.
- Bank will collect KYC documents and basic details of the customer.
  These details will be verified properly before account opening.
- Bank will also understand the nature of customer's work/business and source of income.
  This helps to know whether transactions are normal or not.
- Customers will be classified as Low, Medium or High risk based on their profile.
  This classification helps Bank to decide level of checking required.
- For normal customers, basic KYC and verification is enough.
  Accounts can be opened after proper document checking.
- For high-risk customers (like PEP, NGO, cash business etc.), Bank will do extra checking (EDD).
  Such accounts need approval from higher authority.
- Bank will keep continuous monitoring on transactions after account opening.
  Any unusual or suspicious transaction will be checked.
- If any doubt or suspicious activity is found, Bank will take necessary action as per rules.
  This may include reporting to authorities.
- CDD is not a one-time process, it is continuous during the customer relationship.
  KYC details will be updated from time to time.

## Record Management

Record Management means proper maintenance, storage, and control of all Bank records and documents. The Bank will ensure that all records are kept in a safe, secure, and easily retrievable manner for future reference and compliance purposes.

The Bank will maintain all important records related to customer accounts and banking operations.

- KYC documents, account opening forms, and customer profiles will be properly maintained.
- Records of all transactions, reports, and correspondence will also be preserved.

Records may be maintained in physical or electronic (digital) form as per the Bank's system and facility. Proper security controls will be ensured to protect records from loss, damage, or unauthorized access.

The Bank will preserve records for the period prescribed under RBI and PMLA guidelines.

- Generally, records will be maintained for at least 5 years after closure of account or completion of transaction.
- After the retention period, records will be disposed of in a safe and approved manner.

All records will be made available for audit, inspection, and regulatory requirements whenever required. Any request from auditors or regulatory authorities will be supported with proper documentation.

## Correspondent Banks

- The Bank has correspondent / sponsor banking arrangements with HDFC Bank, IDBI Bank and YES Bank.
- These banks are used for providing payment and settlement services for smooth banking operations.
- The services include UPI, IMPS, NEFT, RTGS, ATM services and other banking facilities.
- These arrangements help in fast, safe and efficient fund transfer and customer services.
- The Bank will ensure that all transactions routed through these banks are properly recorded and monitored.
- All dealings will be done in compliance with RBI guidelines, KYC and AML requirements.
- The Bank will use these correspondent banking services only for legitimate banking purposes and customer transactions

## Risk Categorization

- Bank will classify all customers into Low Risk, Medium Risk and High Risk categories. This is done to understand the level of risk involved with each customer.
- Risk categorization is done based on customer type, occupation, business, location and transaction pattern.
  All types of customers will be covered under this classification.

➢ ***Low Risk Customers***

- Customers like salaried persons, pensioners, small farmers with simple transactions.

- These accounts need normal checking and basic monitoring.

➢ ***Medium Risk Customers***
- Customers like small business, traders, self-employed persons with moderate transactions.
- These accounts need regular monitoring by the Bank.

➢ ***High Risk Customers***
- Customers like PEPs, NGOs/NPOs, trusts, cash-intensive business, complex ownership etc.
- These accounts need extra checking (EDD), approval from higher authority and close monitoring.

## KYC Updating / Risk Review Period

- Low Risk Customers: KYC to be updated once in 10 years. These are normal customers with low transactions.
- Medium Risk Customers: KYC to be updated once in 8 years. These customers have moderate transactions/business.
- High Risk Customers: KYC to be updated once in 2 years. These are sensitive customers and need close monitoring.

## Ongoing Due Diligence

- Ongoing Due Diligence means continuous checking of customer account after opening. Bank should monitor transactions to ensure they are normal and as per customer profile.
- Bank will regularly check account transactions, balance and activity pattern. This helps to identify any unusual or suspicious transactions.
- If any transaction is not matching with customer profile or income, it will be verified. Bank may ask customer for clarification or supporting documents.
- High-risk customers will be closely monitored on regular basis. Extra care will be taken in such accounts.
- Bank will update customer KYC details periodically as per risk category. This ensures customer information is always updated.
- Any suspicious activity found will be reported as per RBI/FIU guidelines. Necessary action will be taken by the Bank.
- Bank will ensure that transactions are consistent with customer's business and source of income.
  Any abnormal activity will be checked immediately.
- Ongoing Due Diligence is a continuous process throughout the customer relationship. It helps in preventing fraud and illegal activities.

## KYC Updation / Periodic Updation

- KYC Updation means updating customer KYC details after a certain period.
  Bank will ensure that all customer information is correct and up to date.
- KYC updation will be done based on risk category:
  - Low Risk – once in 10 years
  - Medium Risk – once in 8 years
  - High Risk – once in 2 years
- Bank may collect:
  - Updated KYC documents, or
  - Self-declaration (if no change), or
  - Use Aadhaar OTP / Digital KYC / other RBI approved methods
- If there is any change in details like address, mobile number, occupation, customer must inform the Bank.
  Bank will update the records after proper verification.
- Bank will send reminders to customers for KYC updation.
  Customer should complete updation within the given time.
- If KYC is not updated on time:
  - Bank may restrict account operations as per RBI rules
  - Transactions will be allowed only after KYC is updated
- Bank will maintain proper records of updated KYC documents.
  These records are required for audit and inspection.
- KYC updation is a continuous process to keep customer details correct.
  It helps in preventing fraud and misuse of accounts.

## CKYC Compliance

CKYC means Central KYC Registry, which is maintained by CERSAI. It is a central system where customer KYC records are stored and can be shared with all banks and financial institutions.

After completing CKYC, the customer gets a unique KYC ID (Identifier). This KYC ID can be used to open accounts in any bank without doing full KYC again.

- Bank will first search CKYC record before doing fresh KYC.
- If CKYC ID is available, Bank will download the KYC details from the system.

If CKYC record is not available, the Bank will create a new CKYC record and upload the customer's KYC details as per RBI guidelines.

- Bank will upload customer KYC data in CKYC system.
- Bank will also update CKYC records whenever there is any change in customer details.

Bank will ensure that all CKYC data is correct, complete and matching with KYC documents. Proper care should be taken while entering and uploading the details.

CKYC helps to avoid repeated KYC process and makes account opening easy and fast. It also improves efficiency and customer convenience.

- Bank will maintain proper records of CKYC upload and download for audit and inspection.
- CKYC system helps in standard process, transparency and better monitoring of customer details.

CKYC also supports compliance and helps in easy verification during audit, inspection and regulatory checks.

## Monitoring of Transactions

Monitoring of transactions means the Bank will regularly check customer account activity to ensure it is normal and as per customer profile.

The Bank will review transactions to identify any unusual, large or suspicious activity. This helps in preventing fraud and misuse of accounts.

- Bank will monitor cash deposits, withdrawals and fund transfers regularly.
- Transactions will be checked based on customer profile, income and nature of business.

If any transaction looks abnormal or not matching with customer profile, the Bank will verify the same.

- Bank may ask customer for clarification or supporting documents.
- High-risk accounts will be closely monitored on continuous basis.

Any suspicious activity will be identified and necessary action will be taken as per rules.

## Issue and Payment of Demand Drafts / Pay Orders

➢ The Bank issues Demand Drafts (DDs) through its sponsor/correspondent banks such as HDFC Bank and IDBI Bank.

- DDs are used for safe fund transfer outside the local area or outside the district/state.
- The Bank issues Pay Orders (POs) within the district/local area where the Bank operates.
- Pay Orders are used for local payments and are payable within the same jurisdiction of the Bank

**Processing and Control**

- All DD/Pay Order issuance will be done as per Bank's internal procedures and RBI guidelines.
- Proper entry and record will be maintained in the system/register.
- Each instrument will have a unique number for tracking and reconciliation.
- Cancellation, re-issue or refund will be processed only after proper verification.

## Reporting Requirements

- The Bank will comply with Prevention of Money Laundering Act (PMLA), 2002 and related RBI guidelines.
- The purpose of reporting is to detect and prevent money laundering and suspicious financial activities.
- The Bank is required to report certain transactions to FIU-IND (Financial Intelligence Unit – India).
- All reports must be submitted within prescribed timelines and in prescribed format.

The Bank is required to report certain transactions to FIU-IND (Financial Intelligence Unit – India) as per PMLA rules.

- CTR (Cash Transaction Report):
  Cash transactions above prescribed limit (₹10 lakh and above) must be reported.
- STR (Suspicious Transaction Report):
  Any suspicious transaction, whether cash or non-cash, must be reported.
- NTR (Non-Profit Organization Transaction Report):
  Transactions related to NGOs/NPOs, if applicable.
- Reports must be submitted within prescribed time limits as per guidelines.
- All reports should be confidential and not disclosed to customer.

The Bank will maintain proper records of all transactions and reports for audit and inspection.

Monitoring and reporting is a continuous process and helps in preventing money laundering, fraud and illegal activities.

## Cash Transaction Reports (CTR)

Cash Transaction Report (CTR) means reporting of high-value cash transactions to the Financial Intelligence Unit – India (FIU-IND) as per PMLA guidelines. The purpose of CTR is to monitor large cash movements and help prevent money laundering activities.

The Bank will identify and report cash transactions as per RBI and FIU-IND requirements.

- Cash transactions of ₹10 lakh and above in a month (single or linked transactions) will be reported in CTR.
- All such transactions will be tracked through the Bank's system and verified properly.

CTR will include both deposits and withdrawals done in cash.

- Large cash deposits in savings, current, or other accounts will be monitored.
- High-value cash withdrawals will also be considered for reporting where applicable.

The Bank will ensure that CTR is prepared and submitted within the prescribed timelines.

- Reports will be submitted to FIU-IND in the required format and time limit.
- Proper records of all reported transactions will be maintained for audit and inspection.

All CTR-related information will be treated as strictly confidential.

- Details of CTR will not be disclosed to the customer or any unauthorized person.
- Staff must handle such information with utmost confidentiality.

## Counterfeit Currency Reports

- Counterfeit currency means fake or forged currency notes that are not issued by the Reserve Bank of India (RBI).
- The Bank is required to identify report and handle counterfeit notes as per RBI guidelines.
- If any fake currency note is detected at the branch, it should be immediately separated and not returned to the customer.
- The details of such notes must be recorded properly in the register/system.

### Reporting Process

- The Bank will prepare a Counterfeit Currency Report and submit it to the concerned authorities as per RBI instructions.
- Such cases may also be reported to police authorities, if required.
- All counterfeit notes should be stamped and kept safely as per RBI procedure.
- Proper acknowledgment should be given where required.

### Politically Exposed Persons (PEPs)

Politically Exposed Persons (PEPs) are individuals who hold or have held important public positions, like ministers, MLAs, government officials, etc. These customers are considered high-risk.

Bank will take extra care while opening and maintaining accounts of PEPs.

- Proper identification of PEP status must be done at the time of account opening.
- Account will be opened only after approval from senior management.
- Bank will do Enhanced Due Diligence (EDD) for such customers.
- Source of funds and income must be clearly verified.
- Transactions in PEP accounts will be closely and regularly monitored.

If any suspicious activity is found, necessary action will be taken as per rules.

**Non-Profit Organizations (NPO/NGO)**

NPO/NGO means organizations working for charitable, social or non-profit purposes. These accounts are also considered sensitive and high-risk in some cases.

Bank will ensure proper verification before opening such accounts.

- Registration documents and legal status of the organization must be verified.
- Purpose and nature of activities should be clearly understood.
- Details of office bearers / trustees / authorized persons must be verified.
- Source of funds and utilization should be checked properly.

Bank will monitor transactions in NPO/NGO accounts carefully.

- Any unusual or large transactions will be verified.
- If required, transactions will be reported as per regulatory guidelines.

These accounts require regular monitoring and proper compliance to avoid misuse.

## Wire Transfer Guidelines

Wire transfer means transfer of funds from one account to another, either within the bank or to another bank. The Bank will ensure that all wire transfers are done as per RBI and AML guidelines.

The Bank must have proper details of both sender and receiver before processing any transfer. This helps in tracking transactions and preventing misuse.

- Bank will collect full details of the sender (remitter) such as name, account number, address or customer ID.
- Bank will also collect details of the beneficiary like name, account number and bank details.

For all transfers, the information should be complete and correct.

- Transfers with incomplete or wrong details should not be processed.
- Such transactions may be rejected or kept on hold for verification.

Bank will monitor wire transfers, especially for large or unusual transactions.

- High-value or suspicious transfers will be checked properly.
- If required, Bank may ask for clarification or supporting documents.

In case of any suspicious transaction:

- Bank will take necessary action and report as per RBI/FIU guidelines.
- Records of all wire transfers will be maintained for audit and inspection.

Wire transfers should be safe, transparent and properly documented. This helps in preventing fraud, money laundering and misuse of banking channels.

## Employee Training & Awareness

Employee Training & Awareness means Bank will regularly train staff on KYC, AML and fraud prevention. This helps staff to understand rules and do their work properly.

The Bank will ensure that all employees are aware of latest RBI guidelines and procedures.

- Bank will conduct regular training programs and workshops for staff.
- Staff will be trained on KYC process, transaction monitoring and reporting requirements.
- Special training will be given to staff handling high-risk accounts and compliance work.

Employees should be able to identify suspicious transactions and activities.

- Staff must report any suspicious matter to higher authority / compliance officer.
- Awareness will be created about frauds, cyber risks and customer safety.

Training is a continuous process to improve staff knowledge and ensure proper compliance.

## Internal Control & Audit

Internal Control & Audit means Bank will have proper system to check and monitor compliance of KYC/AML rules. This helps in identifying mistakes and improving processes.

The Bank will conduct regular audits to ensure all rules are followed properly.

- Internal Audit / Concurrent Audit will check KYC documents and account opening process.
- Audit will verify risk categorization, transaction monitoring and reporting.

Any issues or gaps found during audit will be corrected.

- Branch will take necessary action on audit observations.
- Serious issues will be reported to higher management.

The Bank will maintain proper records and reports for audit and inspection.

- Internal control system helps in preventing fraud, errors and non-compliance.
- It ensures Bank is following RBI and regulatory guidelines properly.

## Customer Education

Customer Education means creating awareness among customers about safe banking practices, KYC requirements and fraud prevention. This helps customers to use banking services safely and avoid fraud.

The Bank will take steps to educate customers from time to time.

- Bank will inform customers about importance of KYC and timely updation.
- Customers will be guided not to share OTP, PIN, passwords or account details with anyone.

Bank will also create awareness about different types of frauds.

- Information will be given about phone frauds, SMS frauds, phishing and cyber frauds.
- Customers will be advised to immediately report any suspicious call or transaction.

The Bank may use different methods to educate customers.

- Display notices in branch and website.
- Send SMS alerts and messages.
- Conduct awareness programs or camps.

Customer education is a continuous process.

- It helps in reducing frauds and protecting customer money.
- It also improves trust and safe banking habits.

## Roles & Responsibilities

Roles and Responsibilities means defining the duties of Board of Directors, Senior Management, Principal Officer and Branch Staff for proper implementation of KYC/AML policy.

All levels in the Bank must ensure that RBI guidelines and internal policy are followed correctly.

➢ ***Board of Directors***

The Board is responsible for overall policy approval and monitoring.

- Approve the KYC/AML Policy of the Bank.
- Review policy periodically and update as required.
- Ensure proper systems and controls are in place.

➢ ***Senior Management***

Senior Management is responsible for implementation of policy.

- Ensure proper execution of KYC/AML policy in all branches.
- Provide guidance and support to staff.
- Monitor compliance and risk management.

➢ ***Principal Officer***

Principal Officer is responsible for AML compliance and reporting.

- Monitor suspicious transactions and activities.
- Report STR/CTR to FIU-IND within time.
- Coordinate with regulatory authorities.

➢ ***Branch Manager / Staff***

Branch staffs are responsible for day-to-day compliance.

- Follow KYC procedures at account opening.
- Ensure proper document verification and record keeping.
- Monitor customer transactions regularly.
- Report suspicious cases to higher authority.

## Reports and Their Periodicity (PMLA Reporting – Co-operative Banks)

The Bank shall submit various reports to FIU-IND as per PMLA guidelines to ensure monitoring of cash and suspicious transactions. The applicable reports for Co-operative Banks are as under:

**1. Cash Transaction Report (CTR)**

- CTR covers cash transactions of ₹10 lakh and above in a month (single or linked transactions).
- It also includes series of cash transactions below ₹10 lakh which are connected within a month.
- All cash deposits and withdrawals in customer accounts will be monitored.

Due Date: CTR must be filed by 15th day of the succeeding month.

**2. Non-Profit Organization Transaction Report (NTR)**

- Covers transactions of NGOs / NPOs involving receipts of ₹10 lakh or more.
- Applicable for accounts maintained in the Bank related to non-profit organizations.

Due Date: As per FIU-IND guidelines (generally along with monthly reporting cycle, if applicable).

**3. Counterfeit Currency Report (CCR)**

- Covers cases where forged or counterfeit currency notes are detected or used as genuine.
- Also includes cases involving forgery of documents or valuable securities used in transactions.

Due Date: To be reported immediately as per RBI / FIU-IND instructions.

**4. Suspicious Transaction Report (STR)**

- Covers all suspicious transactions, whether cash or non-cash.
- Includes transactions that are unusual, not matching customer profile, or suspected for illegal activity.

Due Date: Must be reported within 7 working days after confirming suspicion.

## Use of Technology

Use of Technology means the Bank will use systems and digital tools to improve KYC, monitoring and overall banking operations. This helps in better control, faster processing and reducing manual errors.

The Bank will use technology to ensure proper compliance with RBI guidelines and safe banking.

- Bank will use Core Banking System (CBS) for maintaining customer data and transactions.
- System will help in monitoring transactions and generating alerts for unusual activity.

Technology will be used for KYC processes also.

- Bank may use Aadhaar-based verification.
- CKYC system will be used for uploading and retrieving KYC records.

The Bank will use systems for sanction screening and risk monitoring.

- Customer names will be checked with sanction/negative lists through system.
- High-risk accounts will be tracked and monitored using system alerts.

**Data security is also important.**

- Bank will ensure customer data is safe and confidential.
- Proper controls will be in place to prevent unauthorized access.

## Review of Policy

- The KYC–AML policy will be reviewed at least once every year.
- Review will be done as per latest RBI Master Directions and PMLA guidelines.
- Any new RBI instructions or changes in rules will be updated in the policy immediately.
- Feedback from internal audit, concurrent audit and RBI inspection will be considered.
- Final approval of changes will be given by the Board of Directors.
- The main purpose of review is to ensure updated compliance, proper risk control and safe banking operations.

**The Mahaveer Co-operative Bank Ltd., Belagavi**

Chief Executive Officer/Vice-Chairman/Chairman