

**POLICY ON KNOW YOUR CUSTOMER (KYC)**

**AND**

**ANTIMONEY LAUNDERING MEASURES**

**THE DHANALAKSHMI BANK LIMITED**  
**Central Office: Thrissur**  
**Department: Vigilance**

**VIG/37/2004-05**

**March 19, 2005**

**Policy On Know Your Customer (KYC) and Anti Money Laundering Measures**

The Board in their meeting held on 29.01.2005, has approved this policy of the Bank on 'Know Your Customer (KYC) and Anti Money Laundering Measures' for implementation.

We enclose herewith the copy of this policy along with the modalities to be followed by the staff at supervisory and functional level. All Officers are advised to study the instructions contained therein carefully and implement the same meticulously.

DEPUTY GENERAL MANAGER (INSPECTION)  
&  
MONEY LAUNDERING REPORTING OFFICER  
(MLRO)

## INDEX

	<b>Policy on Know Your Customer (KYC) and Anti-Money Laundering Measures (MML)</b>	
<b>01</b>	<b>Preamble</b>	<b>01</b>
<b>02</b>	<b>Objective</b>	<b>01</b>
<b>03</b>	<b>Chapter I -What is Money Laundering &amp; Back ground</b>	<b>02</b>
<b>04</b>	<b>Appointment of MLRO &amp; DMLRO</b>	<b>03</b>
<b>05</b>	<b>Chapter II – Customer Acceptance Policy</b>	<b>03-06</b>
<b>06</b>	<b>Chapter III- Customer Identification Procedures</b>	<b>06-10</b>
<b>07</b>	<b>Chapter IV- Monitoring of Transactions</b>	<b>10-12</b>
<b>08</b>	<b>Chapter V- Risk Management</b>	<b>12-17</b>
<b>09</b>	<b>General</b>	<b>17-18</b>
<b>10</b>	<b>Modalities of implementing the Policy</b>	<b>19-22</b>
<b>11</b>	<b>(Annexure I ) – Customer Profile for accounts of Individuals - Bio - Data</b>	<b>23-24</b>
<b>12</b>	<b>(Annexure II) - Customer Profile for accounts other than individuals</b>	<b>25-26</b>

THE DHANALAKSHMI BANK LTD  
CENTRAL OFFICE: THRISSUR  
DEPT: VIGILANCE

BANK'S POLICY ON KNOW YOUR CUSTOMER (KYC)  
AND ANTI MONEY LAUNDERING MEASURES (AML)

---

**PREAMBLE**

1.1. Reserve Bank of India has vide their circulars dated 16.8.2002, and 19.9.2002 issued several guidelines on 'Know Your Customer' norms and advised all Banks to follow certain customer identification procedure for opening of accounts and monitoring transactions of suspicious nature for the purpose of reporting it to appropriate authority. RBI has also advised the Banks to put in place the systems and procedures to help control financial frauds, identify money laundering and suspicious activities and to have careful scrutiny/monitoring of large value of cash transactions.

1.2. Reserve Bank of India vide their recent circular dated 29.11.2004, advised all Banks to ensure that a proper policy frame work on 'Know Your Customer' and 'Anti-Money Laundering' measures is to be formulated and put in place with the approval of the Board within three months of the date of this circular, in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Finance of Terrorism (CFT).

**Objective**

1.3. The objective of this policy is to prevent our Branches from being used, intentionally or unintentionally, by criminal elements for money-laundering activities. KYC procedures enable our Branches to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. In tune with the instructions of the Reserve Bank of India, this policy is being dealt with in five chapters as under:

**Chapter I - Introduction, background and appointment of Money-Laundering Reporting Officer (MLRO) and Deputy Money-Laundering Reporting Officer (DMLRO).**

**Chapter II- Customer Acceptance Policy.**

**Chapter III - Customer Identification Procedures.**

**Chapter IV- Monitoring of Transactions.**

**Chapter V- Risk management.**

## CHAPTER – I

### 2. What is Money Laundering?

2.1. **Money laundering is the process whereby proceeds of crimes such as drug trafficking, smuggling (alcohol, arms), kidnapping, gambling, robbery, counterfeiting, bogus invoicing, tax evasion, misappropriation of public funds and the like are converted into legitimate money through a series of financial transactions making it impossible to trace back the origin of funds.** Most often, such clandestine deals are the first step in using the banking system to launder or clean up the cash obtained from trade of illegal goods or services. Once the money is placed within the Bank, it goes through an intricate web of transactions, better known as layering that leave no audit trail. Conversion of this unofficial or black money into official currency thereby 'changing its colour' is called money laundering.

2.2. To launder large sums of unaccountable money, one has to go through the Bank. This is done in three stages described below:

- **Placement** – Physically disposing of cash derived from illegal activities.
- **Layering** - Where the depositor does a series of transactions so that one can not detect the source or link up with the origin of money integration. In short, the process of transferring funds through various accounts to disguise its origin. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.
- **Integration**– Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds. In short, the creation of a legitimate explanation for the source of funds.

### **Background**

2.3. The International Community considers money laundering as a serious crime. Concerted efforts are being made world over to fight money laundering through enactment of stringent laws and regulations and adoption of measures to prevent the financial system being used for laundering proceeds of crime. Considering the global practices in checking Money Laundering, the Governor, Reserve Bank of India desired that a study of the Anti-Money Laundering principles be undertaken by IBA and a code of conduct be prepared for Indian Banks keeping in view of our Banking Provisions and Procedures and Statutory Rules and Regulations. Accordingly, Chairman, IBA constituted a working group under the Chairmanship of Shri P K Sarkar, Deputy Managing Director and Group Executive, International Banking, State Bank of India. The working group consisted of Senior General Managers of various banks made an in-depth study on the measures to be adopted on Anti-Money Laundering Measures by the Banks and submitted a report to the Reserve Bank of India on 31.12.2001.

### **Salient features of the report submitted by the Working Group**

- 2.4. i) Each Bank should have a Board approved policy covering Anti-Money Laundering Measures.
- ii) “Know Your Customer” (KYC) Guidelines may be adopted by the Banks on the lines suggested by the Working group
- iii) Emphasis is laid down on monitoring of transactions for detection of suspicious activities.
- iv) Appointment of Money Laundering Reporting Officer (MLRO) and Deputy Money Laundering Reporting Officer (DMLRO).

Each Bank should appoint a MLRO and DMLRO. They should be officials of sufficient seniority, independence of branch operations, free to act on their own authority and should report directly to the Top Management. It is necessary that the person appointed as MLRO has sufficient operational experience and investigative mind. Both the MLRO and DMLRO are responsible to establish the relevant policies, procedures and controls and ensure their maintenance, which aim to deter criminal elements from using the products and services of the Bank for laundering proceeds of crime. MLRO will be instrumental in activating “Know Your Customer” procedures. MLRO will initiate follow up action on unusual or suspicious activity and co-ordinate with the branch functionaries in deciding on the desirability of continuing the account with increased caution and monitoring or to close the account. They are responsible for preparation of adequate training material for the operating staff and take such steps as necessary to ensure that arrangements are made to train the concerned staff members.

### **Appointment**

- 2.5. In terms of the guidelines and measures suggested, the Deputy General Manager (Inspection) at Central Office is appointed as MLRO and that the Asst. General Manager (Operations) is appointed as DMLRO. The Asst. General Manager (Vigilance) will undertake internal investigations and to have liaison with the Law Enforcement Agencies on receipt of references of suspicious activities from MLRO / DMLRO.

## **CHAPTER – II**

### **3. CUSTOMER ACCEPTANCE POLICY**

- 3.1. For the purpose of KYC Policy, a Customer may be defined as:
- A person or entity that maintains an account and / or has a business relationship with the bank;

- One on whose behalf the account is maintained (i.e. the beneficial owner);
- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

## **Guidelines**

- 3.2. Following are the explicit guidelines given to ensure the customer relationship in the Bank.
- i) No account is opened in anonymous or fictitious /benami name(s);
  - ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk;
  - iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the guidelines issued by Reserve Bank from time to time;
  - iv) Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and/ or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to the bank. Such decision to close an account may be taken at Central Office after giving due notice to the customer explaining the reasons for such a decision, as a built in measure to avoid harassment of those customers;
  - v) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity and
  - vi) Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. Branches are advised to prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social / financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the branch. However, while preparing customer profile, branches should take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

- 3.3. For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc. Customers that are likely to pose a higher than average risk to the bank may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Branches are advised to apply enhanced 'due diligence' measures based on the risk assessment, for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence may include (a) non-resident customers, (b) high net worth individuals, (c) trusts, charities, NGOs and organizations receiving donations, (d) companies having close family shareholding or beneficial ownership (e) firms with 'sleeping partners', (f) politically exposed persons (PEPs) of foreign origin, (g) non-face to face customers and (h) those with dubious reputation as per public information available etc. It is important to bear in mind by the branches that its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

#### **Accounts of Politically Exposed Persons (PEPs) resident outside India**

- 3.4. Politically exposed persons are individuals or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state owned Corporation, important political officials, etc. The branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. The branches should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP should be taken at Central Office level. The branches should also subject such accounts to enhanced monitoring on an on-going basis. The above norms are applicable to the accounts of the family members or close relatives of PEPs also.

## **Correspondent Banking**

- 3.5. Correspondent Banking is the provision of Banking Services by one Bank (the correspondent Bank) to another Bank (the respondent bank). These services may include cash/funds management, international wire transfers, drawing arrangements for Demand Drafts and Mail transfers, payable through accounts, cheques clearing, etc. The branches should gather sufficient information to understand fully the nature of the business of the respondent bank. Information on the other Bank's management, major business activities, purpose of opening the account, identity of any third party entities and regulatory/supervisory frame work in the correspondent's country may be of special relevance. Similarly, the branches should try to ascertain from publicly available information whether the other Bank has been subject to any money laundering or terrorist financing investigation or regulatory action. Such relationship should be established only with the approval of the Board. The Board may delegate the power to a Committee headed by the MD & CEO of the Bank while laying down clear parameters for approving such relationship. Proposals approved by the committee should invariably be put up to the Board for post facto approval.
- 3.6 In the case of payable – through accounts, the branches should satisfy that the respondent Banks have verified the identity of the customers having direct access to the accounts and is undertaking on-going 'due diligence' on them. Branches should also ensure that the respondent Bank is able to provide the relevant customer identification data immediately on request.
- 3.7 The branches should refuse to enter into a correspondent relationship with a 'shell bank' (a Bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). The Branches should also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks. The branches should be extremely cautious while continuing relationship with respondent banks located in countries with poor KYC standards and countries identified as 'non co-operative' in the fight against money laundering and terrorist financing .

## **CHAPTER – III**

### **4. CUSTOMER IDENTIFICATION PROCEDURES**

#### **What is Identity?**

- 4.1 Customer **identification** means identifying the customer and verifying his/her identity by using reliable independent source documents data or information. The Branches need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer and the purpose of the intended nature

of banking relationship. Due diligence is to be observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to Banks and a burdensome regime for the customers.

4.2. For customers who are natural persons, the branches should obtain sufficient identification data to verify the identity of the customer, his address/location and also his recent photograph. For customers who are legal persons or entities, the branches should (i) verify the legal status of the legal person/entity through proper and relevant documents, (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person and (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

### **Introduction / Identification of Accounts**

4.3 Identification of a customer and introduction by an acceptable person are important pre-requisites for opening an account. No account is opened for any person without proper introduction or verification of the identity of the person. Careless handling of the matter may give room for undesirable customers to commit frauds, misappropriation and deceive the general public. Necessary precaution and strict adherence of norms in this respect can be a check on the activities of miscreants trying to defraud the Banking System.

### **What is Identification?**

4.4 Identification is the act of establishing who a person is. In the context of KYC (Know your Customer), identification means establishing who a person purports to be. This is done by recording the information provided by the customer covering the elements of his identity (i.e. name and all other names used, and the address at which they can be located). Following are some of the documents which the branches can accept for establishing identity of a person:

- Passport
- Driving License
- Identity Card of any Institution
- PAN Card
- Voter's Identity Card
- Other documentary evidence in support of the person's residential address in addition to the above.
- 

### **What is Verification?**

4.5 Verification of identity is the process of proving whether a person actually is who he claims to be. In the context of KYC, verification is the process of seeking satisfactory evidence of the identity of those with whom the branch does business. This is done by carrying out checks on the correctness of the information provided by the client. The best available evidence of identity should be obtained, having regard to the circumstances of each client and their country of origin. Some forms of proof

of identity are more reliable than others, and in some case it will be prudent to carry out more than one verification check.

### **Guidelines on Introduction**

4.6 Branches generally insist on “introduction” by a known person. Introduction is a process of ascertaining the identity of a person and his acceptability for establishing business relationship. Before opening an account, the branches must get true identity of the intending customer verified. When the branch opens an account in the name of a customer, it has to render a number of services, including collection of cheques, in the ordinary course of business. It is, therefore, essential that the branch is aware of the credentials of the prospective customer such as his profession, business address, etc. Proper introduction and verification of antecedents of account holder in each and every account are, therefore, essential.

### **What is a Proper Introduction?**

4.7. It is necessary that the person introducing the applicant to the branch must himself be a respectable person. He should also be known to the Banker. The introducer should know the intending customer. The introducer should sign bank’s forms in token of his verifying the identity of the applicant. Oral introduction of a person desirous to open an account with the bank would not constitute a proper introduction.

4.8. KYC Guidelines go beyond merely establishing the identity of the person and satisfying about his credentials. The due diligence expected under KYC invokes going into the purpose and reasons for opening the account, anticipated turn-over in the account, source of wealth (net-worth) of the person opening the account and the source of funds flowing into the account. While opening new accounts, the branches in addition to routine procedures, make their efforts to get documents for identification and proof of residence having present and permanent addresses along with telephone numbers etc., from the account-openers. Particulars of other accounts with any other banks, Permanent Account Number (PAN) given by Income Tax Authorities, Registration Certificate in the case of partnership firms and Certificate of Incorporation, Memorandum & Articles of Association from Companies and Resolution by Boards for accounts of Companies should be obtained. The branches should prepare a customer profile containing the expected activities of his business. They should collect additional details such as:-

- Employment details such as job specifications, name and address of the employer, length of service etc.;
- Details about source of income and annual income;
- Details of assets owned such as house, vehicle etc;
- Other personal details such as qualification, marital status etc.

This profile would give an idea of the expected transactions in the account as assessed /envisaged at the time of opening of the account. Any suspicious activity can be compared with this profile.

#### 4.9 Features to be verified and documents to be obtained from customers

Features	Documents
<p><b>Accounts of individuals</b></p> <p>Legal name and any other names used.</p> <p>Correct permanent address</p>	<p>(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence. (v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of branch.</p> <p>(i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Letter from employer (subject to satisfaction of the branches) (any one document which provides customer information to the satisfaction of the branch will suffice)</p>
<p><b>Accounts of Companies</b></p> <p>Name of the company</p> <p>Principal place of business</p> <p>Mailing address of the company</p> <p>Telephone/Fax Number</p>	<p>(i) Certificate of incorporation and Memorandum &amp; Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill.</p>
<p><b>Accounts of partnership firms</b></p> <p>Legal name</p> <p>Address</p> <p>Names of all partners and their address</p> <p>Telephone numbers of the firm and partners.</p>	<p>(i) Registration certificate if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses and (v) Telephone bill in the name of firm/partners.</p>

<p><b>Accounts of trusts &amp; foundations</b></p> <p>Names of trustees, settlers, beneficiaries and signatories.</p> <p>Names and addresses of the founder, the managers/directors and the beneficiaries.</p> <p>Telephone/fax numbers.</p>	<p>(i) Certificate of registration, if registered  (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlers and their addresses. (iv) Resolution of the managing body of the foundation/association and (v) Telephone bill.</p>
--	---

## CHAPTER - IV

### **5. MONITORING OF TRANSACTIONS**

5.1 The objectives of the KYC frame work are in two folds, (i) to ensure appropriate customer identification and (ii) to monitor transactions of a suspicious nature. It should be ensured that the procedure adopted does not lead to denial of access to the general public for banking services. Ongoing monitoring is an essential element of effective KYC procedures. The branches can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extend of monitoring will depend on the risk sensitivity of the account. The branches should pay special attention to all complex, unusually large transactions and unusual patterns which have no apparent economic or visible lawful purpose. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the branch. The branches should take note that high account turn over inconsistent with the size of the balance maintained may indicate that funds are being ‘washed’ through the account. The branches should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

#### **5.2 An indicative list of suspicious activities**

- a) Corporate accounts where deposits or withdrawals are primarily in cash.
- b) Corporate accounts where deposits, withdrawals and remittances, transfers from/made to sources apparently unconnected with the corporate business activity/dealings.
- c) Unusual applications for D.D/T.T./P.O. against cash.
- d) Accounts with large volume of credits through D.D./T.T./P.O.
- e) A single substantial cash deposit composed of many high denomination notes.
- f) Frequent exchanges of small denomination notes for large denomination notes or vice-versa.
- g) Multiple accounts under the same name and sudden surge in activity level.
- h) Sending or receiving frequent or large volumes of cross border remittances.

- i.) Remittances received by T.T./D.D./P.O. from various centers and in turn remitting the consolidated amount to a different account/centre on the same day leaving minimum balance in the account.

### 5.3 **Monitoring Procedure**

- i) Branches are required to issue traveller's cheques, demand drafts, mail transfers and telegraphic transfers for Rs.50,000/- and above only by debit to customers' accounts or against cheques and not against cash received. Branches should ensure to get the Permanent Account Number of the customer /applicant while issuing demand drafts/pay orders for amount Rs.10,000/- and more. If the applicant is not an account holder, a photo copy of the PAN Card should be filed with the application.
- ii) Branches are required to keep a close watch on cash withdrawals and deposit of Rs.10 lakhs and above in deposit, cash credit or overdraft accounts and keep record of details of these large cash transactions in a **separate register**.
- iii) Branches are required to report all cash deposits and withdrawals of Rs.10 lakh and above as well as transactions of suspicious nature with full details in fortnightly statements to their controlling offices. Besides, controlling offices are also required to apprise Central Office regarding transactions of suspicious nature. All Zonal/Group Offices should report these transactions to the Deputy Money Laundering Reporting Officer at Central Office, who would consolidate and report the transactions to the 'Top Management'.

### **Internal Control System**

- 5.4 Duties and responsibilities should be explicitly allocated for ensuring that policies and procedures are managed effectively and that there is full commitment and compliance to an effective KYC programme in respect of both existing and prospective deposit accounts. Zonal/Group Offices will periodically monitor strict adherence to the laid down policies and procedures by the officials at the branch level.

### **Terrorism Finance**

- 5.5 Lists of terrorist entities, as notified by the Govt. of India, are communicated to all the Zonal/Group Offices, so that branches may exercise caution if any transaction is detected with such entities. The branches should ensure that such lists are consulted with their controlling authorities in order to determine whether a person/organization involved in a prospective or existing business relationship appears on such a list. Branches should report accounts suspected to belong to terrorist entities or transactions of suspicious nature, to the Deputy Money Laundering Reporting Officer at Central Office.

### **Internal Audit/Inspection**

- 5.6 i) An independent evaluation of the controls for identifying high value transactions should be carried out on a regular basis by the internal audit Dept.

- ii) Concurrent/ internal auditors to specifically scrutinize and comment on the effectiveness of the measures taken by branches in adoption of KYC norms and steps taken towards prevention of money laundering.

#### 5.7 **Adherence to Foreign Contribution Regulation Act (FCRA), 1976**

- i) Branches should also adhere to the instructions on the provisions of the Foreign Contribution Regulation Act, 1976 cautioning banks to open accounts or collect cheques only in favour of foreign organizations, which are registered under the Act by Govt. of India. A certificate to the effect that the organization is registered with the Govt. of India should be obtained from the concerned foreign organizations at the time of opening of the account or collection of cheques.
- ii) Branches should exercise due care to ensure compliance and desist from opening accounts in the name of banned organizations and those without requisite registration.

#### 5.8. **Record Keeping**

In the case of wire transfer for transactions, the records of electronic payments and messages must be treated in the same way as other records in support of entries in the accounts. All financial transactions records should be retained for at least five years after the transaction has taken place and should be available for perusal and scrutiny of audit functionaries as well as regulators as and when required.

#### 5.9 **Training of staff and management**

All the operating and management staff should fully understand the need for strict adherence of KYC norms. Hence there should be ongoing training programme so that staff members are adequately trained for their roles and responsibilities in complying with Anti-Money Laundering guidelines and for implementing KYC policies consistently. The training shall review applicable money laundering laws and recent trends in money laundering activity with reference to our Bank's policies and procedures to combat money laundering including how to recognize and report suspicious transactions.

## **CHAPTER – V**

### **6. RISK MANAGEMENT**

#### 6.1 **Definition of Risk Management**

‘Risk is the result of uncertain future’. Risk Management is identification, measurement, monitoring and control of risks by systematic actions, in a planned manner, through proper understanding and communication.

## 6.2 Risk Management system in the Bank.

In tune with the Reserve Bank of India guidelines for management of Credit, Market and Operational risk, our Bank has adopted a separate Risk Management Policy as per our Bank's requirements based on size, complexity of business, market perception and capital adequacy requirements and the same was approved by the Board. The salient features of this policy are given below:

## 6.3 Organisation and set up

(a) Risk Management is a Board driven function. At present the Asset – Liability Management Committee, (ALCO) of senior executives headed by the Chairman (ALCO) deals with different types of market risks. RBI has suggested the formation of Credit Policy Committee of senior executives to oversee issues relating to credit policy and procedures and to analyse, manage and control credit risk. RBI has also suggested that Banks could set up a single committee for integrated management of credit and market risks. Since the composition of the two committees would be more or less the same, the Board has considered it desirable to have a single committee in place. This will enable the participants to take care more balanced view of the affairs of the Bank. The composition of the committee which may be otherwise called as the Risk Management Committee consist of the following members.

- i) Managing Director & CEO.
- ii) Executive Director.
- iii) Head of Risk Management Department.
- iv) Head of the Credit Department.
- v) Head of Operations Department.
- vi) Head of the Planning Department.
- vii) Head of the Human Resources Department (By invitation).

The quorum would be three with the presence of either the MD & CEO or the ED being obligatory.

(b) A separate Risk Management Department headed by an Officer is already created and functioning. This department is responsible for policy, control and monitoring of all market risks and credit risk..

(c) The objective in introducing the Risk Assessment System is to put in place a tool for an ongoing assessment of risk elements inherent in Bank's advances so that the operating functionaries would be regularly put on alert and appropriate measures could be initiated to reduce/eliminate risk.

#### 6.4 Status of Risk Management Process

The risks faced by Bank of our type and size have been broadly categorized as :

- Credit Risk
- Market Risk
- Operational Risk

#### 6.5 Credit Risk Management

(a) The revised Credit Policy of the Bank has been approved by the Board at their meeting held on 26.6.2004 . The revised scheme for delegation of financial powers for advances and bank's policy on Unsecured Exposures were also approved by the Board in their meeting held on 06.7.2004. The policies have been circulated to all operating personnel who were advised to study the instructions carefully and implement the same meticulously.

(b) Delegation of powers for undertaking lending and non-lending business has been put in place.

( c ) Loan Review mechanism for an independent review of credit risk assessment with the aim to bring improvement in the quality of credit portfolio is in place.

(d) Prudential exposure limits of counter party exposure for banks and other borrowers, groups, industry etc. as per RBI guidelines are in place.

(e) Credit Risk Measurement process is in tune with the regulatory requirements such as selection criteria, credit appraisal, approach to interest rates on advances, follow up, supervision, monitoring and control, periodicity of inspection etc. have been put in place.

(f) With Risk Rating System in place, monitoring of Bank's advances from the risk angle becomes easy for risk management at corporate level. It also helps functionaries at Zonal/Group/Branch levels as a barometer of risk and helps to initiate appropriate remedial measures in the case of individual borrowers. Further, at macro level, the bank can restrict or expand credit exposure to industries depending on risk perceptions.

(g) Non-managing credit risk has two consequences both individual and systemic. Credit risk management has two basic objectives. One is to manage the asset portfolio in a manner that ensures that our bank has adequate capital to hedge their risks. The other is to match the returns to the risks.

(h) Effective credit risk assessment allows our bank to reduce risk and potential NPAs. Once the branches understand their risks and cost, they will be able to determine the most profitable business, and price products according to risks.

- (i) The threat of bad loans rears its head through the entire credit cycle. There are five crucial areas that Credit Risk Management should focus on:
- a. Periodically inspect collaterals to check gradual erosion in value.
  - b. Build information system that continuously track credit risk.
  - c. Monitor concentration of exposure across the product portfolio.
  - d. Tackle Non-Performing loans quickly and effectively.
  - e. The branches and controlling offices need to play a much more active role regarding our customers by analysing their businesses, insisting on better disclosures and discouraging them from meaningless expansion as well encouraging them to improve their operational efficiency.
- (j) With a view to overcome the deficiencies/constraints, credit evaluation systems need to be geared up to develop differential pricing across the various categories of borrowers. Pricing is now mainly dependent on Credit Risk Assessment (CRA) even though value of an account is an indispensable factor that also goes on to determine the price. Credit exposure with high risk goes with stiff pricing. It is, therefore, necessary that credit officers/appraisers use the CRA technique very carefully and diligently to arrive at the correct risk rating so that the pricing determined on the basis of the CRA is appropriate to the level of risk and does not adversely affect Bank's earnings. In view of the criticality of CRA from the income angle, it is necessary that our officials handling credit proposals fully equip themselves with the CRA technique and Bank's guidelines in the matter.
- (k) The pricing for fund-based facilities under CRA, albeit influenced by the relative risk rating of a unit, is also determined with reference to several other business factors / strategic reasons. There may, thus cases where actual pricing of a fund-based facility is consciously fixed at above/below the indicative spread flowing from the risk ratings. To illustrate, an account rated as A may not, ipso facto merit a Prime Rate. In such cases, the risk ratings should not be disturbed. It would also be necessary to seek approval of the pricing of the loan from the sanctioning authority in the proposal itself, should this be different from that indicated by the risk rating, adding due reasons thereof. In as much as the CRA introduces certain qualitative facets of the Company's managerial aspects and involves judgmental assessment on sensitive issues, the method of computation of rating need not be disclosed to the customer and/or to the participating banks in the consortium, if any. Only the pricing of the facility is to be indicated/negotiated.
- (l) A summary of the risk rating should accompany the loan proposal. The Bank has a Credit Rating System for exposures exceeding Rs.50 lacs. At present this rating is being used mainly for determining the interest spreads, with higher rates being stipulated as the rating goes down. The system will continue to be used for pricing the asset.

(m) Once the internal rating system stabilizes, the tracking of the rating over a period will provide valuable clues in respect of the progress or the decline in the borrower's standing. A negative movement will alert the bank towards taking defensive action to protect its interest.

(n) It should be the endeavour to ensure that limits of borrowers enjoying the top three risk ratings constitute at least 60% of the total limits. Since the risk rating is at present extended to customers with limits exceeding Rs.50 lacs, this stipulation will also apply to the same group of accounts.

(o) The Bank had engaged the services of ICRA Advisory Services for suggesting improvements in the credit management processes. ICRA in the first stage had made a preliminary study of our portfolio, which is in line with RBI recommendation on CRM. The first phase was marked as the "diagnostic phase". The second phase, the "Prescriptive phase" mainly portfolio to build up healthy assets. In line with their recommendation, the bank has adopted a comprehensive loan application form and appraisal forms for trade/industrial credit large advances.

## 6.6 Market Risk

(a) Asset Liability Management Committee (ALCO) of senior executives headed by the Chairman (ALCO) deals with different types market risks.

(b) Market Risk Management inter alia Risk Mitigating Tools, Take over advances, Loan Syndication, working capital facilities, corporate loans, bill discounting facilities, lease financing, secured term loans, non-fund facilities such as letters of credit, private placement of debentures, placement of commercial paper and valuation of securities are dealt with in detail in the Bank's Credit Policy document.

## 6.7. Operational Risk Management

(a) Guidelines for internal control, system and procedures for various business segments are already in place. These controls inter alia include segregation of duties, reporting system as well as various other checks and balances.

(b) Organisational structure at Central Office, Zonal/Group Offices and branches has been clearly defined. The role and responsibilities, reporting lines etc., have been defined in systematized manner.

(c) Manual of instructions for various segments of banking business viz. deposits, remittances, cash and clearing, Advances, Foreign Exchange and miscellaneous are updated and written guidelines/instructions are issued from time to time.

(d) System of credit audit and stock audit for compliance of terms of sanction/system of vetting of documents by advocates, monitoring of weak assets on the basis of early warning signals is in place. Similarly written instructions/guidelines on stock statements, stock audit, inspection, insurance etc. are issued to branches from time to time.

(e) Full fledged independent inspection headed by a Dy General Manager for ongoing monitoring of the system of internal control by conducting inspection /audit of the branches is functioning in the bank.

(f) **Information technology:** Instructions regarding Security, Back up and Disaster Recovery for strict compliance are issued from time to time by Central Office. A policy on Business Continuity Plan has already been prepared and is in the process of getting approval from the Board.

(g) **Anti-Money Laundering Controls:** Detailed instructions on 'Know Your Customer' issued by RBI have been communicated to all branches, Zonal/Group Offices for strict compliance. The present policy on Anti-Money Laundering Controls is put up before the Board for getting approval.

(h) Fraud Risk Management Policy 2004 -05 to bring about awareness and prevention of frauds is also in the process of getting approval from the Board.

## **7. General**

7.1 Concurrent/internal auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard may be put before the Audit Committee of the Board on quarterly intervals.

7.2 The Inspection and Audit Departments have an important role in evaluating and ensuring adherence to the KYC policies and procedures.

7.3 The in-house Training College should have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements should have different focuses for dealing with new customers. Needless to emphasise that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

### **7.4 Customer Education**

Implementation of KYC procedures requires the branches to demand certain information from customers which may be of personal nature or which has hitherto never been called for. This may lead to sometimes a lot of questioning by the customer as to the motive and purpose of collecting such information. The customers should be educated about the objectives of KYC programme by issuing specific literature/pamphlets etc. The staff needs to be specially trained to handle such situations while dealing with the customers.

### **7.5 KYC for the Existing Accounts :**

Branches are advised to comply with the instructions/guidelines issued by RBI vide their circulars dated 16.8.2002, 24.11.2003, 16.12.2003, and 21.6.2004 in respect of applying

the KYC norms to all the existing customers in a time bound manner. The branches should monitor the transactions in the existing accounts of any unusual pattern in the operation. It should be ensured that all the existing accounts of Companies, firms, trusts, charities, religious organizations and other institutions are subjected to minimum KYC standards which would establish the identity of a natural /legal person and those of the 'beneficial owners'. The branches may also ensure that term/recurring deposit accounts or accounts of similar nature are treated as new accounts at the time of renewal and subjected to KYC procedures. Where the branch is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-cooperation by the customer, the branch may consider recommending closure of the account or terminating the banking/business relationship explaining the reasons for taking such a recommendation. Final decisions need to be taken at Zonal Office/Group Office level.

**Modalities of Implementing Bank's Policy on Know Your Customer (KYC) and Anti Money Laundering Measures (AML)**

In tune with the guidelines prescribed by RBI vide their Circular reference DBOD.No.AML.BC.58/14 01-001/2004-05 dated 29.11.2004, a separate policy on KYC & AML was prepared and the same was approved by the Board during its meeting held on 29.01.2005. The modalities of implementing the guidelines laid down in the policy Vis –a - Vis the detailed guidelines given by RBI in this subject are furnished below.

**2. Need for prevention of Money – Laundering Activities.**

2.1. To protect Bank from

- a) Reputation Risk.
- b) Operation Risk. (where chances of fraud come to light)
- c) Legal Risk. (Leads to legal battle.)
- d) Concentration Risk. (affects Balance Sheet)
- e) Compliance Risk. (non-compliance leads to penalties)

2.2. It is obligatory on each bank as per the Prevention of Money Laundering Act 2002 to provide Audit trail and to report the Suspicious Activities and Cash transactions involving Rs.10 lakhs and above to the RBI. Probing of such transactions and respective customers is to be looked into by the investigative and law enforcement agencies.

**3. Customer Profile**

3.1. As part of Customer Acceptance Policy and Monitoring of suspicious Transactions (laid down in the main policy), each branch has to prepare the 'Risk Profile' of each customer and classify them as Low Profile Customer (level - I) Medium Profile Customer ( Level- II) and High Profile Customer (Level – III) based on the location, turnover, socio-economic status and based on the Risk Categorization mentioned herein below. The branch should exercise 'due diligence' while monitoring the transactions based on the data collected.

<b>Risk Categorization</b>	<b>Description</b>	<b>Level of due diligence to be applied</b>
Low Risk (Low Profile customer)	Salaried Accounts, Customers and firms with low income turnover, Agricultural Customers, Accounts of Government Departments, PSUs, Regulatory bodies, SEBI etc. Customers having credit –debit summation of below Rs.10 lakhs in a year.	Basic level.
Medium Risk (Medium Profile Customer)	Customers, Companies and firms having turn over of above Rs.10 lakhs and up to Rs. 50 lakhs in their accounts.	Enhanced level.
High Risk (High Profile Customer)	Companies, Institutions and Firms having turn over of Rs.50 lakhs and above in their accounts.	Enhanced level.

3.2 Customer Profile for **Individuals** should be compiled after having interactive session with each customer covering the following information also in addition to the data already collected while opening the account. A separate format has been devised and furnished in **Annexure I**. The Officer, authorizing the opening of the account should prepare the customer profile in the given format and sign the document. The customer profile contains information relating to customer identity, social/financial status, nature of business activity, information about his business and their location etc. It is to be noted that the customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

- i) Social / financial status.
- ii) Names and addresses of close relatives.
- iii) Source of funds for credit to accounts.
- iv) Monthly Income.
- v) Annual Turnover
- vi) Dealings with other Banks / Financial institutions.
- vii) Anticipated Level of Transactions with Bank.

3.3. Similarly, Customer Profile **for other than individuals** should be compiled covering the following additional information in the format prescribed separately and furnished in **Annexure II**. The officer authorizing the opening of the account should prepare the profile and sign the document.

- (i) Nature of Business
- (ii) Major Customers and Suppliers.
- (iii) Source of Funds.
- (iv) Details of Beneficial Owners.
- (v) Details of Promoter Directors and major share holders with names, addresses and percentage of share.
- (vi) Details of Office Bearers with names and addresses.
- (vii) Copy of latest financial statement and Income Tax Return..

#### **4. Monitoring of Transactions.**

- Unusual and large value of Cash Transactions.
- Transactions of suspicious nature.
- Terrorism Finance.

#### **Cash Transactions:**

4.1. All Branches are advised to exercise 'due diligence' in the process of monitoring of transactions based on customer profiles prepared. In case of suspicious activities branches should exercise 'enhanced due diligence' and arrange to report then and there. The entire approach is Risk Based. For instance, if there is a sudden increase of deposit in an account from Rs.10,000/- to Rs.50 lakhs and above, the branch should be in a position to give satisfactory explanation before the Law Enforcement Agencies. Such transactions are to be reported to the Controlling Office immediately.

4.2. It is mandatory on the part of all branches to issue TC's, DD's, MT's and TT's for Rs.50,000/- and above only by debit to customer's account or against cheques but not against cash.

4.3. The branches should insist the customers to affix PAN on the applications for the above referred transactions for amounts of Rs.50,000/- and above.

4.4. All branches should open a separate Register (if not done already) for recording cash withdrawals and deposits of Rs.10 lakhs & above and monitor such transactions followed by reporting to respective Zonal / Group offices.

4.5. All Branches are advised to monitor transactions of just below the threshold limits fixed above and submit reports to the controlling authority.

#### Transactions of suspicious nature

4.6. The branches should look for unusual / irregular suspicious transactions. If the business activity goes out of the activity already declared by the customer and compiled in the customer profile and the transactions though apparently found legal and if there is no business logic, such transactions are to be monitored as suspicious. An indicative list of suspicious activities has been furnished in page 10 para 5.2. of the policy document. The same is reproduced herein below for ready reference.

#### **An indicative list of suspicious activities**

- a) Corporate accounts where deposits or withdrawals are primarily in cash.
- b) Corporate Accounts where deposits, withdrawals and remittances, transfers from/made to sources apparently unconnected with the corporate business activity/dealings.
- c) Unusual applications for DD/TT/PO against cash
- d) Accounts with large volume of credits through DD/TT/PO.
- e) A single substantial cash deposit composed of many high denomination notes.
- f) Frequent exchanges of small denomination notes for large denomination notes or vice versa.
- g) Multiple accounts under the same name and sudden surge in activity level.
- h) Sending or receiving frequent of large volumes of cross border remittances.
- i) Remittances received by TT/DD/PO from various centre and in turn remitting the Consolidated amount to a different account/sender on the same day leaving minimum balance in the account.

#### Terrorism Finance

4.7. Lists of terrorist entities as notified by the Government from time to time are communicated to all Branches / Zonal / Group Offices so that branches should exercise caution if any transaction is detected with such entities. This has also been dealt with in the policy document vide page No. 11, Para 5.5

### **5. Reporting System**

#### Control Reports / Returns.

5.1. The Board has approved the nomination of Deputy General Manager (Inspection) as the Bank's Money Laundering Reporting Officer (MLRO) and the Assistant General Manager (Operation) as the Deputy Money Laundering Officer (DMLRO). All the branches controlling offices and the MLRO / DMLRO at Central Office, should follow the time limit prescribed here under to report the Cash Transactions of Rs.10 lakhs and above and also the transactions of Suspicious Activities by way of sending separate Suspicious Activity Report (SAR) to the respective authorities noted against each.

<b>Subject</b>	<b>Authorities to report</b>	<b>Existing system</b>	<b>New system to be adopted</b>
To report Cash Transactions of Rs.10 lakhs and above and the transactions just below the threshold limit	Branches to Zonal / Group Offices	Fortnightly basis (on or before 15 <sup>th</sup> of every month)	Same system to continue.
To report suspicious Cash Transactions of Rs.10 lakhs and above and the transactions just below the threshold limit	Controlling offices to MLRO /DMLRO at Central Office	After scrutiny of branch statements, controlling offices are sending reports to Inspection Dept. at Central Office to the effect that there is no suspicious transactions. No time limit is fixed.	The same system of reporting should continue but on quarterly basis (on or before 10 <sup>th</sup> of January, April, July, & October.
Suspicious Activity Report (SAR) i.e. Transactions of suspicious nature	Branches to Zonal / Group Offices.	Other than cash transaction of Rs.10 lakhs and above, no system of sending suspicious activity report.	To report as and when detected by SAR
Suspicious Activity Report (SAR) i.e. transactions of suspicious nature	Controlling Offices to MLRO / DMLRO, at Central Office.	Other than cash transaction of Rs.10 lakhs and above, no system of sending suspicious activity report.	To report as and when detected by SAR

**CUSTOMER PROFILE FOR ACCOUNTS OF INDIVIDUALS****Bio-data**

1.	Name	:	
2.	Date of Birth	:	
3.	Height	:	
4.	Complexion (mention whether dark, wheatish or fair)	:	
5.	Educational qualification	:	
6.	Hobbies & Interest	:	
7.	Occupation (Whether employed or self employed or own business. If so, nature of business/line of activity)	:	
8.	Mobile/Telephone No.	:	
9.	Religion	:	
10.	Permanent Address	:	
11.	Name of		
	Father (with address & telephone No.)	:	
	Mother (with address & telephone No.)	:	
12.	Social/Financial status (Whether occupying any political post or leader of any religious organization/office bearers of any Trust/ Social organization etc. e.g. Panchayat President, President/General Secretary of Lions Club etc.)	:	

13.	Source of Funds for credit to accounts	:
14.	Monthly income (Approximate) (a) Transactions in the form of cash (b) Transactions in the form of cheques/DDs/Pay Orders © Transactions in the form of Credit Cards	:
15.	Annual Turnover (Approximate)	:
16.	Existing credit facilities	:
17	Anticipated level of transactions with the Bank	:

**Note:**

The officers authorizing the opening of the account should prepare the customer profile in the format prescribed above and sign the document. The officers should concentrate in collecting all the information required especially in the areas mentioned above as serial Nos.12,13,14,15,16 and 17. All officers/Managers are advised to see that the information appearing in the Account Opening Form should tally with the information collected while preparing the customer profile.

Annexure –II

## Customer Profile for Accounts other than individuals

1.	Name of the constituent	:
2.	Nature of constitution (Proprietary/Partnership/HUF/Others/Club/Association Private Ltd./Public Limited	:
3.	Name & address of the proprietor/Partner/Directors/Office bearers with Telephone/Mobile Numbers	:
4.	Nature of business/ Line of activity	:
5.	Description of business activity	
6.	Names of major customers and suppliers with their telephone numbers	:
7.	Source of Funds	:
8	Details of beneficial owners (Name, address & Telephone No.)	:
9.	Details of promoter Directors (Names, address and telephone Nos.)	:
10	Details of major share holders (Names, addresses telephone No. and percentage of share)	:
11	Details of office bearers in case of Associations, Unions, Trust etc – Names address and telephone Nos.)	:

13	Copy of Income Tax Return obtained (Yes/No). If no, reasons to be furnished	:
14	Approximate Monthly Turnover (a) Extent of cash transactions (approx.) (b) Extent of transactions by cheque/DD/Pay Order © Extent of transactions by other mode like credit cards/debit cards etc.	:
15	Anticipated level of transactions with Bank	:

Note:

The officers authorizing the opening of the account should prepare the customer profile in the format prescribed above and sign the document. The officers should concentrate in collecting all the information required especially in the areas mentioned above at serial Nos. 4, 5, 6, 11,12,13,14 and 15. All officers/Managers are advised to see that the information appearing in the Account Opening Form should tally with the information collected while preparing the customer profile.