एन आई सी एशिया बैंक लि.

Policy for

Prevention of Money Laundering

And

Combating the Financing of Terrorism

2016

NIC ASIA Bank Limited

Policy for Prevention of Money Laundering and Combating the Financing of Terrorism 2016

In exercise of the power conferred by Section 14(2) of Bank and Financial Institution Act 2063 and the Articles of Association of NIC ASIA Bank, the Board of Directors of NIC ASIA Bank has approved this "Policy for Prevention of Money Laundering and Combating the Financing of Terrorism- 2016" vide its 262nd Board Meeting dated January 26, 2016 for implementation after review and recommendation of 40th meeting dated January 11, 2016 of Risk Management Committee of the Bank. The core purpose of this policy document is to lay down a framework for prevention of money laundering and combating financing of terrorism, and provide guidelines on AML/CFT compliance across all the functions of the Bank.

Version History

S. No.	Version	Approving Authority	Date of Approval
1	1st	Board of Directors	March, 2007
2	2nd	Board of Directors	September 15, 2014
3	3rd	Board of Directors	January 26, 2016

Approval Sheet

Initiated By	Santosh Kunwar Senior Assistant- IRMD	(Original Signed)
Reviewed & Supported By	Roshan Kumar Neupane Chief Risk Officer	(Original Signed)
Reviewed By	Dipak Dhakal Manager Internal Audit	(Original Signed)
Reviewed By	Bishal Sigdel Manager- Finance	(Original Signed)
Reviewed By	Sushil Bhattarai Manager – IT	(Original Signed)
Reviewed By	Parmeswor Shrestha Manager IT-SAP	(Original Signed)
Reviewed By	Dinesh Bhari Head Legal and Corporate Affairs	(Original Signed)
Reviewed By	Sudhir Pandey Chief Operating Officer	(Original Signed)
Reviewed By	Bhanu Dabadi Head-Human Resource	(Original Signed)
Supported By	Laxman Risal ACEO	(Original Signed)

Contents

Chapter-I: General

1. Background, Short Title, and Commencement

Anti-Money Laundering (AML) has developed to be of significant importance for financial institutions around the world. The many allegations and revelations that BFIs are used as a vehicle for providing financial services to money launders and terrorists garnered enormous impetus to curb channeling of money derived from crime or aimed at funding terrorism. Moreover, governments are pursuing reforms in regulatory structures and are also cracking down on tax evasion to recover lost revenue. The stringent provisions made in laws and directives reflect the seriousness of this issue; non-compliance of which may cause significant reputational risk as well as may result in adverse consequences for the Bank. Regulators have also been closely monitoring the AML/CFT policies, procedures, guidelines and practices of financial institutions.

In order to prevent the Bank from being used for money laundering and financing of terrorism, the Board of Directors of NIC ASIA Bank has approved this policy. This policy has laid down appropriate framework for effective compliance to Asset (Money) Laundering Prevention Act 2061, Anti (Money) Laundering Prevention Rules, 2066 and Directives issued by Financial Information Unit (FIU) and Nepal Rastra Bank (NRB) from time to time

This Policy shall be known as the “Policy for Prevention of Money Laundering & Combating Financing of Terrorism”.
It shall come into force from the date it is approved by the Board.

2. Definitions

Unless otherwise specifically indicated, the following terms used in NIC ASIA Bank Policy for Prevention of Money Laundering and Combating the Financing of Terrorism-2016 shall have the following meaning(s):

a. Money Laundering
Money laundering is the process by which the person attempt to hide and disguise the true origin and ownership of the proceeds of their unlawful activities. The term” Money Laundering” is also used in relation to the financing of terrorist activity (where the funds may, or may not, originate from crime).

b. Financing Terrorism

Financing of Terrorism means providing financial support to any form of terrorism or to those who encourage terrorism.

c. Customer Due Diligence (CDD)

Customer Due Diligence is the process of identifying and evaluating the customer and re-assessment of customer risk as part of know your customer (KYC) process, allowing banks to better identify, manage, and mitigate the AML related risks.

d. Simplified Customer Due Diligence (SCDD)

Simplified Customer Due Diligence is the process of identifying and evaluating the low risk graded customer.

e. Enhanced Customer Due Diligence (ECDD)

Enhanced Customer Due Diligence refers to additional due diligence pertaining to the identity of the customer, source of income, nature and value of transaction etc. for customer transactions other than low risk graded.

f. Financial Action Task Force (FATF)

The FATF is an inter-governmental body which sets standards, and develops and promotes policies to combat money laundering and terrorist financing. It currently has 36 members jurisdictions and 2 regional organizations: and more than 20 observers: five FATF-style regional bodies and more than 15 other international organizations or bodied. The purpose of the FATF is to develop policies to combat money laundering and terrorism financing. The FATF Secretariat is housed at the headquarters of the OECD in Paris. In response to mounting concern over money laundering, the Financial Action Task Force on Money Laundering (FATF) was established by the G-7 Summit that was held in Paris in 1989. Recognizing the threat posed to the banking system and to financial institutions, the G-7 Heads of State or Government and President of the European Commission convened the Task Force from the G-7 member States, the European Commission and eight other countries.

g. Financial Information Unit (FIU)

In order to work against the money laundering and terrorist financing activities Financial Information Unit (FIU) was established on April 21, 2008 pursuant to section 9 of the Assets (Money) Laundering Prevention Act, 2008 within Nepal Rastra Bank (the Central bank) as an independent unit. It is Nepal's financial intelligence unit. It is a central, national agency responsible for receiving, processing, analyzing and disseminating financial information and intelligence on suspected money laundering and terrorist financing activities.

h. Asia/Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organization founded in 1997 in Bangkok, Thailand consisting of 41 members and a numbers of APG. Some of the key international organizations who participate with, and

support the efforts of the APG in the region include the Financial Action Task Force, International Monetary Fund, World Bank, OECD, United Nations Office on Drugs and Crime, Asian Development Bank and the Egmont Group of Financial Intelligence Units.

APG members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the Forty Recommendations of the Financial Action Task Force on Money Laundering (FATF).

i. Shell Entity

Shell Entity is a company that is incorporated but has no assets or operations. A Shell Entity serves as a vehicle for business transactions without having any significant assets or operations of its own Shell corporations in themselves may not be illegal as they may have legitimate business purposes. However, they can also be a main component of underground activities, especially those based in tax havens.

One of the classic tax avoiding activities can be buying or selling of Shell Companies established in tax havens to disguise actual profits. Furthermore a firm can carry out its international operations through these types of entities and not report to its home country about the sum involved and thereby avoid tax.

j. Vendors

The term Vendor, for the purpose of this document, denotes any third party who supplies the Bank with any product through transfer of ownership and with whom such purchases is made by the Bank contract.

Other than the terms specifically defined hereinabove, the terms used in various sections of this Policy shall have the same meaning as has been defined under various other policy documents of the Bank and the applicable laws of land, wherever relevant.

3. Objectives of the Policy

The major objectives of the policy are:

- To lay down a framework to be implemented by the Bank in order to safeguard it against being used for money laundering and financing of terrorism:
- To ensure full compliance by the Bank with all applicable legal and regulatory requirements pertaining to money laundering and financing of terrorism,: and
- To provide a board framework for formulation and implementation of various manuals or procedural guidelines that is required for effective AML/CFT & KYC compliance.

4. Money Laundering and Financing of Terrorism

4.1 Money Laundering

The financial Task Force on Money Laundering defines the money laundering as:
"The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money Laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source.

Illegal arms sales, smuggling, and the activities of organized crime including for example drug trafficking and prostitution rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimize" the ill-gotten gains through money laundering.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

In response to mounting concern over money laundering, the Financial Action Task Force on money laundering (FATF) was established by the G-7 Summit in Paris in 1989 to develop a co-ordinate international response. One of the first tasks of the FATF was to develop Recommendations, 40 in all, which set out the measures national governments should take to implement effective anti-money laundering programs".

4.2 Financing of Terrorism

Terrorist financing involves the solicitation, collection or provisions of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. More precisely, according to the International Convention for the Suppression of the Financing of Terrorism, a person commits the crime of financing of terrorism "if the person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an offense within the scope of the Convention.

The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity.

4.3 Money Laundering Process

The Money Laundering consists of the following processes:

4.3.1 Placement

In the initial or placement stage of money laundering, the launders introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposit directly, into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.

4.3.2 Layering

After the funds have entered the financial system, the second- or Layering – stage take place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channeled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

4.3.3 Integration

Having successfully processed his criminal profits through the first two phases of the money laundering process, the launderer then moves them to third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

4.4 Money Laundering Areas

As money laundering is a necessary consequence of almost all profit generating crime, it can occur practically anywhere in the world. Generally, money launders tend to seek out areas in which there is a low risk of detection due to weak or ineffective anti-money laundering programs. Because the objectives of money laundering is to get the illegal funds back to the individual who generated them, launderers usually prefer to move funds through areas with stable financial systems. Therefore, Banks have been the targets for money launderer.
Money laundering activity may also be concentrated geographically according to the stage the laundered funds have reached. At the placement stage, for example, the funds are usually processed relatively close to the under-lying activity: often but not in every case, in the country where the funds originate.

With the layering phase, the launderer might choose an offshore financial center, a large regional business center, or a world banking center – any location that provides an adequate financial or business infrastructure. At this stage, the laundered funds may also only transit bank accounts at various locations where this can be done without leaving traces of their source or ultimate destination.

Finally, at the integration phase, launderers might choose to invest laundered funds in still other locations if they were generated in unstable economies or locations offering limited investment opportunities

One of the latest trends in money laundering involves use of the new payment technologies like Smart Cards, Online Banking, and Electronic Cash etc. The Bank should be vigilant and should administer the robust controlling, monitoring and reporting system to Prevent money laundering and financing of terrorism through such channels.

5. Regulatory and Supervisory Requirements

5.1 International Perspectives

The Original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering typologies. The 1996 Forty Recommendations have been endorsed by more than 130 countries and are the international anti-money laundering standard.

The Forty Recommendations now apply not only to money laundering but also to terrorist financing, and when combined with the Nine Special Recommendations on Terrorist Financing provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing. The FATF recognizes that countries have diverse legal and financial systems and so all cannot tale identical measures to achieve the common objectives, especially over matters of detail. The Recommendation therefore set minimum standards for action for countries to implement the detail according to their particular circumstances and constitutional frameworks. The Recommendations cover all the, measures that national systems should have in place within their criminal justice and regulatory systems: the preventive measures to be taken by financial institutions and certain other businesses and professions: and international co-operation.

The major highlights of revised 40 FATF recommendations issued on 2012 are listed below:

A – AML/CFT Policies and Coordination

1 – Assessing risks & applying a risk-based approach
2 – National cooperation and coordination

B - Money Laundering and Confiscation

3 – Money laundering offence
4 – Confiscation and Provisional measures

C – Terrorist Financing and Financing for Proliferation

5 – Terrorist financing offence
6 – Targeted financial sanctions related to terrorism & terrorist financing
7 – Targeted financial sanctions related to proliferation
8 – Non-profit organizations

D – Preventive Measures

9 – Financial institution secrecy laws

Customer due diligence and record keeping

10 – Customer due diligence
11 – Record Keeping

Additional measures for specific customers and activities

12 – Politically exposed persons
13 – Correspondent banking
14 – Money or value transfer services
15 – New technologies
16 - Wire transfers

Reliance, Controls and Financial Groups

17 - Reliance on third parties
18 - Internal controls and foreign branches and subsidiaries
19 – Higher-risk countries

Reporting of suspicious transactions

20 – Reporting of suspicious transactions
21 - Tipping-off and confidentiality

Designated non-financial Businesses and Professions (DNFBPs)

22 – DNFBPs: Customer due diligence

23 – DNFBPs: Other measures

E – Transparency and Beneficial Ownership of legal Persons and Arrangements

24 – Transparency and beneficial ownership of legal persons
25 – Transparency and beneficial ownership of legal arrangements

F – Powers and Responsibilities of Competent Authorities and other institutional measures

Regulation and Supervision

26 – Regulation and supervision of financial institutions
27 - Powers of supervisors
28 - Regulation and Supervisions of DNFBPs (Designated non-financial Businesses and Professions)

Operational and Law Enforcement

29 – Financial intelligence units
30 – Responsibilities of law enforcement and investigative authorities
31 – Powers of law enforcement and investigate authorities
32 – Cash couriers

General Requirements

33 – Statistics
34 – Guidance and feedback

Sanctions

35 – Sanctions

G – Internal Cooperation

36 – Internal instruments
47 – Mutual legal assistance
38 – Mutual legal assistance: freezing and confiscation
39 – Extradition
40 – Other forms of international cooperation

The major highlights of nine special recommendations made by FATF are as follows:

1. Ratification and implementation of UN instruments

2. Criminalizing the financing of terrorism and associated money laundering
3. Freezing and confiscating terrorist assets
4. Reporting suspicious transactions related to terrorism
5. International co-operation
6. Alternative remittance
7. Wire Transfers
8. Non- profit organizations
9. Cash couriers

The recommendations of FATF shall be taken care of by the Bank as applicable.

Besides the FATF, following bodies are also functional:

- The Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)
- The council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) (formerly PC-R-EV)
- The financial Action Task Force on Money Laundering in South America (GAFISUD)
- Middle East and North Africa Financial Action Task Force (MENAFATF)
- Eurasian Group (EAG)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Intergovernmental Action Group against Money-Laundering in West Africa (GIABA)
- The International Monetary Fund (IMF)
- The World Bank

5.2 Applicable Legal Framework

The applicable domestic legal frameworks pertaining to AML/CFT are as follows:

a. Anti-Money Laundering Act, 2064 (Including amendments)
b. Anti-Money Laundering Rules, 2066:
c. Unified Directives No. 19 issued by Nepal Rastra Bank:
d. Directives/Guidelines issued by FIU (Directives to implement UNSCR (United Nations Security Council Resolutions) 1267 & 1373, Directives to Banks & Financial Institutions, Suspicious Transactions Reporting Guidelines & Threshold Transactions Reporting Guidelines)

The Legislation pertaining to the AML/CFT mandates the FIU to:

- Receive/collect reports on financial transaction that are of suspicious nature and/or above the prescribed threshold and other information relevant to money laundering and

financing of terrorist activities from government agencies and financial and non-financial institutions,

- Analyze and assess information received from the reporting agencies,
- Provide relevant information to the concerned investigation department and other relevant units,
- Direct banks, Financial and non-financial institution on the reporting requirements,
- Ensure compliance by reporting entities with regard to their obligations under the law, rules and regulations,
- Inspect transaction and records of banks, financial and non-financial institutions,
- Manage training and awareness programs
- Take actions against banks, financial and non-financial institutions in case of non-compliance of reporting requirements, and
- Develop information exchange mechanisms with other FIUs or related international institutions by entering into formal understandings or obtaining memberships.

Chapter-II: Bank's Policy and Framework for AML/CFT and KYC Compliance

6. NIC ASIA Bank's Policy on prevention of Money Laundering & Financing of Terrorism

In order to protect the Bank's reputation and to meet its legal and regulatory obligations, it is of utmost significance that the Bank safeguards it against the risk of being used for money laundering and financing of terrorism.

The Bank's policy on the prevention of money laundering and financing of terrorism shall apply to all the branches and businesses of the Bank.

As an organization committed to the prevention of money laundering and financing of terrorism, the Bank will:

- Establish clear lines of internal accountability, responsibility and reporting

- Document, implement and maintain **procedural guidelines** which interpret**/implement this** policy and set standards for each business **in line with** the law, regulations and regulatory guidelines. Compliance with such procedures and **guidelines** will be monitored regularly by the Compliance Unit.

- Take all reasonable steps to verify the identity of customers, including the beneficial owners of corporate entities (including Trusts), and the principles behind customers who are acting as agents. The Bank will take all reasonable steps to ensure that " Customer Due Diligence" information is collected and kept up-to-date, and that identification information is updated when changes come to the Bank's notice regarding the parties involved in a relationship
- Establish procedures to retain adequate records of identification, account opening and transactions. Identification, account opening records and transaction records shall be retained for minimum seven years after a relationship has ended. Records relating to internal and external suspicious transactions reports should also be retained for a minimum of seven years

- Refuse/Report any transaction where, based on explanations offered by the customer or other information, reasonable grounds exist to suspect that the funds may not source from a legitimate source or are to be used for an illegal activity or as to be used for financing of terrorism or if customer/applicant/beneficiary refuses or fails to submit required information/ documents.

- Make prompt reports of suspicious transactions, or proposed transactions or any other money laundering and financing of terrorism issues through the internal channels as prescribed by the Bank from time to time to the relevant authorities as required by statutory regulations,

- Raise awareness through periodic and regular trainings on money laundering and financing of terrorism among employees covering what money laundering and financing of terrorism is the methods of recognizing suspicious transactions, the regulatory requirements and the procedures and controls adopted by the Bank to control/prevent money laundering and financing of terrorism and other relevant matters,

- Co-operate with any lawful request for information made by authorized Government Agencies/Statutory Bodies during their investigations into money laundering and financing of terrorism

- Support Government Statutory Bodies and law enforcement agencies in their efforts to combat the use of the financial system for the laundering of the proceeds of crime or the movement of funds for criminal purposes.

- Not maintain any kind of relationship with “Shell Banks/Shell Companies” (“Shell Bank/Shell Company” is a bank/company without a physical presence). The Bank will also exercise due diligence in establishing correspondent relationships with local/foreign banks.

- Not ‘tip-off” its customers regarding suspicious transactions and/or any internal/external investigation being carried on them.

- Install adequate system of checks and internal control to prevent the money laundering and combat the financing of terrorism, and

- Treat the issues pertaining to the money laundering and financing of terrorism as “Zero Tolerance Issues” and take action as a high priority issue.

7. AML/CFT and KYC Compliance Framework

NIC ASIA Bank's Anti Money Laundering & Combating Financing of Terrorism standards are designed to help the businesses meet their responsibilities in relation to the prevention of money laundering &financing of terrorism. These standards are primarily based on the relevant laws/regulations, regulatory/statutory guidelines and the best practices on prevention of money review based on the changes on the relevant laws/regulations/statutory guidelines,

NIC ASIA Bank's Anti Money Laundering & Combating Financing of Terrorism standards are based on the following nine standards:

- **Governance and Oversight**
- **Internal Controls**
- **Risk Assessment**
- **Risk Based Customer Due Diligence**
- **Selective Transaction and Sanction Screening**
- **Transaction and Account Surveillance**
- **Reporting Suspicious Transactions**
- **Training and Awareness**
- **Independent Testing**

The standards set by this document are applicable to all business/branches. If a business/branch is unable to apply the standards set by this documents (in exceptional circumstances), the matter must be immediately raised with the Chief Operating Officer, Chief Risk Officer, and AML implementing Officer and any deviation from these standards must have pre-facto approval of the **DCEO/CEO**.

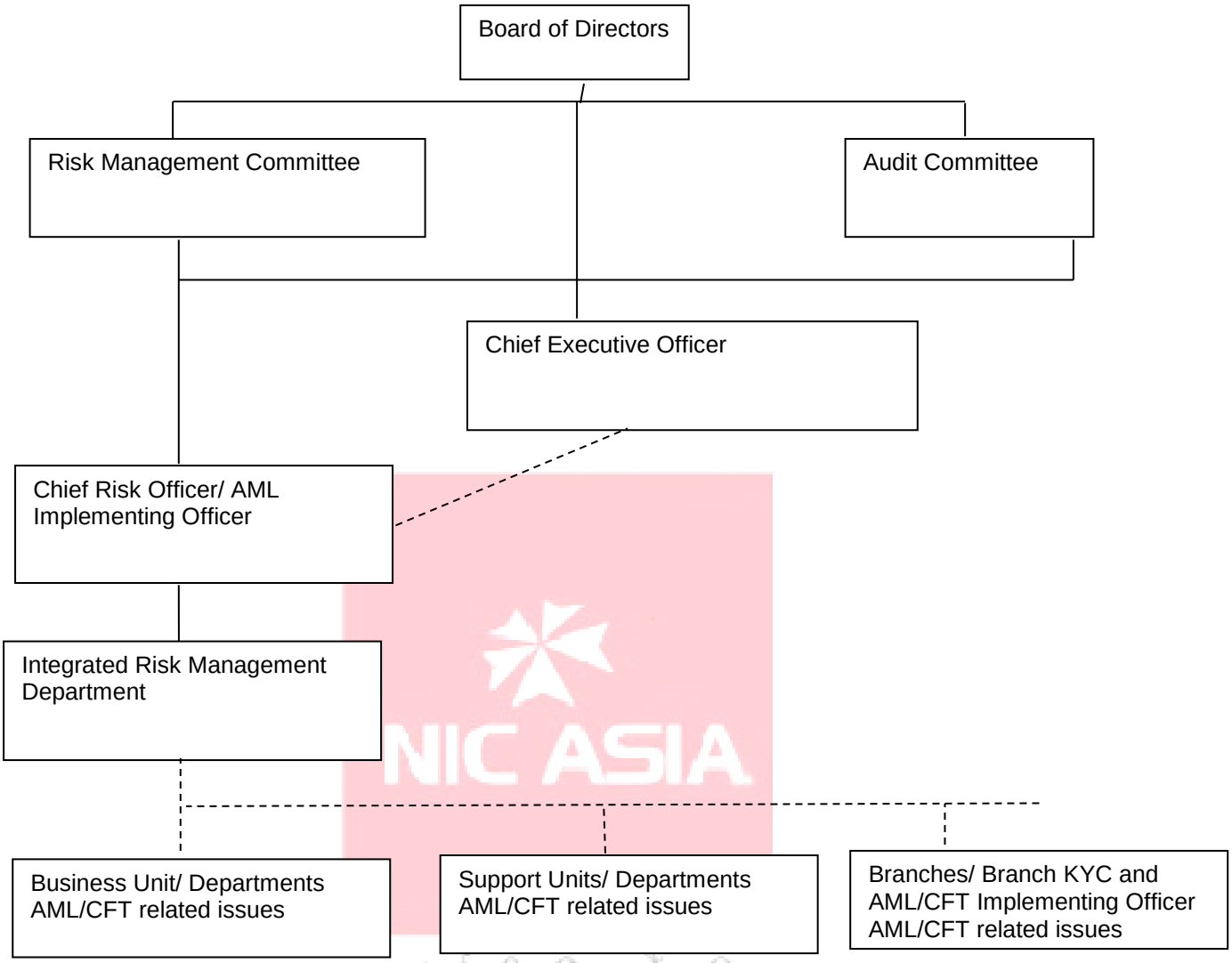
7.1 Governance and Oversight

7.1.1 AML/CFT Unit and AML/ Implementing Officer

The Bank shall have an AML/CFT Unit under its Compliance function under the purview of Chief Risk Officer. An **AML Implementing Officer** shall be appointed to function as a focal point for implementation of this policy, and guidelines formulated to execute in practice this policy, Acts, rules and regulations, and directives from regulatory body regarding Anti-Money Laundering and Combating the Financing of Terrorism.

The AML Implementing Officer of the Bank shall put forth quarterly update on the AML/CFT and KYC compliance of the Bank for deliberation at Risk Management Committee and the Board of Directors of the Bank.

The reporting organogram for issues pertaining to AML/CFT compliance shall be as postulated in the following diagram.



AML Implementing Officer shall be responsible for the general oversight of the Bank's policy for Prevention of Money Laundering & Combating Financing of Terrorism effectiveness of the control, monitoring and reporting procedures and to establish and maintain adequate arrangements for training on prevention of money laundering and financing of terrorism. She/he shall also be responsible for ensuring prompt response to queries from internal/external authorities and for assisting Business Units/Branches in meeting their responsibilities as described herein above. Para 8 of the FIU Directives to Banks & Financial Institution lists down the following responsibilities of AML implementing Officer:

a) To perform and cause to perform activities as required to be followed by the reporting institution under Anti-Money Laundering Act Rules directive order circular issued under the said Act as well as other related statutes.

b) To identify the customer as required by the legal instruments including the Asset (Money) Laundering Prevention Act and rules, directives, order circular issued under the said Act.
c) To maintain and cause to maintain updated record of Customer Due Diligence information as per point no. b)
d) To properly maintain the record of transaction exceeding the threshold and suspected transactions
e) To submit information of transactions as per point no. (d) to Financial Information Unit within the stipulated time .

The obligations of the AML Implementing Officer as prescribed in Rule 10 of the Anti-Money Laundering Rules are as follows:

a) Function as focal point to perform tasks in accordance with the Act, these Rules and the Directives,

b) Cause to maintain secure record of transaction,

c) Provide information about suspicious or other necessary transaction to the Financial Information Unit through letter or electronic means of communication like fax, email, etc.

d) Provide information about transaction of the branch offices to the Financial Information Unit in a regular basis.

The details of AML implementing officer like name, address, qualification, contact number, email etc. shall be furnished to FIU and information regarding the change in AML implementing officer and details thereof shall also be notified to FIU.

7.1.2 Branch KYC and AML/CFT Implementing Officer:

The Chief Executive Officer upon recommendation of Chief Risk Officer shall appoint Branch AML/CFT & KYC Officer for each Branch of the Bank. The Branch KYC and AML/CFT Implementing Officer shall have a direct reporting line to the country AML Implementing Officer for AML/CFT related issues. For all the other matters, incumbent shall report to the respective segment Heads.

7.2 Internal Controls

The Bank shall have adequate procedures and processes to ensure effective checks, reviews and controls in executing AML/CFT and KYC Compliance. The Bank shall have defined procedures for the following activities:

1. Transaction and Account Surveillance;
2. Reporting;
3. Customer Identification, Acceptance and Due Diligence;
4. Sanction Program and AML Database (PEPs, HNW and other Adverse Media);

5. Assessment of KYC Compliance; and
6. Training on AML/CFT

The operating manuals, product paper guidelines, procedural guidelines, standard operating procedures etc. formulated by the Bank shall address under a separate section the provisions of AML/CFT Compliance and assessment of ML/FT risks unique to the product or the function.

7.3 Risk Assessment of Money Laundering/ Terrorism Financing Threats and Vulnerabilities

The Bank shall carry out Risk Assessment of threats and vulnerabilities related to money laundering and terrorism financing as required by the Assets (Money) Laundering Prevention Act 2064 and its subsequent amendments, NRB Unified Directive19 and its subsequent amendments, and AML Rules 2066. The Risk Assessment helps to identify and assess threats and vulnerabilities in the Bank's operating environment pertaining to Money Laundering and Terrorism Financing and thereby the risks the Bank is susceptible inherent to money laundering and terrorism financing.

The risk assessment shall be carried out for:

- ML/FT risks in products,
- ML/FT risks in services,
- ML/FT risks in delivery methods
- ML/FT risks in customer base (nature and type) ,

The Risk Assessment shall be carried out annually and the risk assessment report shall be presented to Risk Management Committee. The annual Risk Assessment report shall be submitted to Financial Information Unit, Nepal Rastra Bank as required by Unified Directives 19 and amendments there to.

7.4 Risk Based Customer Due Diligence and Due Diligence of Vendors and Business Partners

Customer Due Diligence (CDD) (which includes Simplified Customer Due Diligence (SCDD) and Enhanced Customer Due Diligence (ECDD)) shall be the fundamental tool of achieving the goals set by this policy document on "Prevention of Money Laundering & Combating the Financing of Terrorism" based on the risk grading of the customer. CDD shall be carried in such a way that it not only establishes proper customer identification, but also helps in understanding the nature of business of a relationship. CDD shall be an ongoing process and shall continue even after the account opening procedures are completed so that it can reduce the risk of accounts being used for money laundering & financing of terrorism and can help the Bank to identify suspicious transactions and can also guard the Bank against frauds and forgeries.

- CDD shall be relevant across all of the Bank's business. The reference made below therefore includes all types of relationships with customers.

- In order to enable the Bank to use CDD as a fundamental tool for prevention of money laundering, the following CDD information must be held in file:

    - Full customer identification evidence (including address verification evidence)
    - The reason for the relationship recorded with sufficient detail to provide an understanding of the purpose of the account and the nature of the customer's business or employment.
    - An indication of the anticipated volume and type of activity to be conducted through account
    - Bank's understanding of the source of funds routed through the account
    - Recording of the underlying source of wealth in case of High Net Worth accounts.

The Bank shall have a risk based customer due diligence program incorporating:

1. Customer Identification Process
2. Periodic Review of Customer Due Diligence
3. Customer Due Diligence based on Risk Category

7.4.1 Meaning of Customer

The person or entity that maintains account or someone on whose behalf an account is maintained with a Bank or Financial Institution or those on whose behalf an account is maintained i.e. beneficial owners is called customer. Any person or entity connected with a financial transaction that may impose significant reputational or other risks to the Bank or Financial Institution is also considered as customer for the purpose of these documents e.g. walks in customers requesting for one-off transaction. As per circular /Directives issued by NRB, Customer includes persons who are (or who seek to be):

- In a business relationship
- Engage in one or more occasional transactions
- Involved in carrying out wire transfer as prescribed in Circular/Directives issued by NRB
- Engage in any business or transaction in any instance where there is a suspicion that the person is involved in money laundering or terrorist financing with the bank and financial institution.

7.4.2 Customer Identification Process

Customer Identification Process (CIP) is a critical part of Customer Due Diligence process. It is essential to establish the true identity (and address) of the customers and

that the customers are not conducting business in factious names, possibly to disguise their involvement in illicit/illegal activities. While identifying the natural person or legal person, the Bank shall obtain the documents, data and information as prescribed. All the documents and information pertaining to the identification of the natural person or legal person, the Bank shall obtain the documents, data and information as prescribed. All the documents and information pertaining to the identification of the natural person or legal person should be retained in a legible/understandable manner and in the managed way.

Reasonable step must therefore be taken by obtaining sufficient evidence of identify, to be able to establish true identify of customers. When a customer is acting (or appears to be acting) on behalf of other (for example as agent), sufficient identification evidence must be obtained in respect of both parties (i.e. agent and the principal behind agent). These steps must be taken as soon as possible after contact with a customer or potential customer is made with a view to carrying out a transaction or establishing a relationship.

All customer accounts and relationships shall be graded into three KYC risk categories according to the assessment of level of KYC risk they carry. These risk categories are Low KYC Risk Account/Relationships, Medium KYC Risk Account/Relationships, and High KYC Risk Account /Relationships. Customer due diligence should be carried on the basis of risk profile of the customers. Enhanced Customer due diligence should be applied for high risk customer and simplified customer due diligence should be applied for low risk customers.

The provisions of Customer Due Diligence should also be duly addressed in the credit appraisal of the customers that the Bank has a lending relationship with.

7.4.3 Periodic review of Customer Due Diligence

CDD information shall be regularly reviewed even after the completion of account opening or the commencement of a relationship. The frequency of reviews shall be determined by the level of risk associated with the relationship and recorded as part of the customer file data. Higher risk, high value or high volume accounts shall, for example, be reviewed at more frequent intervals.

Any shortcomings in CDD information highlighted by a review must be corrected as soon as possible. Steps must be taken to obtain additional information about existing customers where it is apparent that existing CDD information is out of date or inadequate.

Any information on change in the ownership and/or change in persons controlling a relationship or any other worthy/requiring information shall be taken as a trigger to update CDD information.

7.4.4 Customer Due Diligence based on Risk Category

The procedural guidelines framed under this Policy shall summarize CDD and identification standards for the all the customer categories across the Bank. For any customer category, whether or not specified by such Guidelines, CDD and identification procedures adopted must be in line with this policy document and the regulatory guidelines.

7.4.5 Due Diligence of vendors, service providers and business partners

The Bank shall have in place the tools and procedures for identification of vendors, service providers and business partners in alignment with the KYC norms from AML perspectives.

The procedural guidelines framed under this policy shall incorporate the due diligence standards for:

i. listed vendors and service providers from whom the Bank purchases, rents, or avails service through bidding as per the Bank's Financial Administration By laws;
ii. individuals, firms, companies or organizations hired by the Bank for consulting;
iii. individuals, firms, companies or organizations that the Bank enters into a contract with whereby a party to the contract acts as an agent of the another;
iv. individual, firms, companies or organization that the Bank enters into a contract with as a business partner ;
v. Financial and non-financial institutions that the Bank's establishes a relationship in the course of its business.

The Bank shall not maintain any relationship with the party where:

i. legitimacy of the party is undeterminable;
ii. the party proffers false, misleading or substantially incorrect information;
iii. the party refuses to disclose and/or to provide documentation related to identity and nature of business;
iv. the party refuses to provide the identification of beneficial owners;
v. the party is a shell entity;
vi. the party requests redemption of the fees to be transferred to an off shore location or to a jurisdiction identified by FATF to be a non-cooperative jurisdiction; and
vii. the party or the parent of the party or a subsidiary of the party is incorporated in a jurisdiction identified by FATF to be a non-cooperative jurisdiction.

7.5 Selective Transaction and Sanctions Screening

The Bank shall not maintain relationships with the prohibited customer types and shall not carry out prohibited transactions types outlined in this Policy. The Bank shall deploy sanction

screening programs to safeguard itself from maintaining relationship or carrying out transaction in which a party to the transaction is a sanctioned entity.

7.5.1 Prohibited Customer Types

The Bank shall not carry out transactions or maintain any relationship with the following customer types:

1. Shell Banks
2. Shell Entities
3. Offshore Banks
4. Entities (including natural person, legal person, vessels etc.) sanctioned by major sanction authorities such as United Nations, Office of Foreign Assets Control- United States, Her Majesty's Treasury-United Kingdom, etc.

7.5.2 Prohibited Transactions Types

It is the policy of the NIC ASIA Bank to avoid the following transactions:

1) Payment orders with inaccurate representation of the person placing the order,
2) Acceptance of payment remittances from other banks without indication of the name or account number of the beneficiary;
3) Use of accounts maintained by the bank for technical reasons, such as sundries accounts or transit account, or employees' accounts to filter or conceal customer transactions;
4) Maintaining accounts under pseudonyms that are not readily identifiable;
5) Opening Accounts without name or with notional name;
6) Acceptances and documentation of collateral that do not corroborate with the actual economic situation or documentation of fictitious collateral for credit granted on trust;
7) Providing customer or third parties, at the customers' request, with incomplete or otherwise misleading documents or information in connection with the customer's accounts; and
8) Providing Downstream Correspondent Banking.

7.5.3 Sanction Screening:

The Bank shall instigate a control measure for safeguarding the Bank against being used as a conduit for Money Laundering and Financing of terrorism by individuals/entities listed in the Sanction List published by UN, OFAC, HMT-UK etc.

The procedure developed under this document for screening of customers/ beneficiaries/ originators before opening of a customer account and execution of cross-border transaction such as payments through Swift/Draft/ RTGS/NEFT/VA/TT etc. shall ensure that the Bank has a robust customer acceptance and payment system immune to risks arising from ML/TF risks associated with Sanctioned Individuals and Entities. Such screening mechanism shall also include the existing customer database sweep against sanction list.

7.6 Transaction and Account Surveillance

Effective ongoing monitoring is vital for understanding of customer's activities and an integral part of effective AML/CFT system. It helps to know the customers and to detect unusual or suspicious activities.

The business relationship with a customer should be continuously monitored by:

- Reviewing from time to time, documents, data and information relating to the customer to ensure that they are up-to-date and relevant,

- Monitoring the activities (including cash and non-cash transactions) of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds, An unusual transaction may be in the form of activity that is inconsistent with the expected pattern for that customer, or with the normal business activities for the type of product or services that is being delivered and

- Identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate AML/CFT.

Ongoing monitoring of the business relationship should be conducted on a risk sensitive and appropriate basis.

Business Units/Units and Branches must monitor compliance with the policy, standards, legal and regulatory requirements, procedures and controls through the tools as prescribed through separate Guidelines/Manuals and the results of such monitoring shall be shared with the AML Implementing Officer. These results shall form the basis of a continuing process to improve the overall anti-money laundering & combating financing of terrorism control process including training requirements.

7.7 Reporting Suspicious Transactions

Guideline for Detecting Suspicious Transaction issued by FIU states that "Suspicious Transaction Reports (STRs) include detailed information about transactions that are or appear to be suspicious. The goal of STRs filings is to help the Financial Information Unit (FIU) of Nepal identify individuals groups and organizations involved in fraud, terrorist financing, money laundering, and other crimes. The purpose of a STR is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the provision related Asset (Money) Laundering Prevention Act, 2008.

FIU requires an STR to be filed by a financial Institution when the financial institution suspects insider abuse by an employee, violations of law or more that involve potential money laundering or violation of existing AML/CFT law, or when a financial institution knows that a customer is operating as an unlicensed money services business.

The general characteristics of suspicious financial transaction as mentioned in Guidelines for Ducting Suspicious Transaction issued by Financial Information Unit (FIU) are as follows:

1. Transactions having unclear economical and business target,
2. Transaction conducted in relatively large amount cash and/or conducted repeatedly and unnaturally.
3. Transaction conducted differently from that of usually and normally conducted by the relevant customer.
4. Huge, complex and unusual transaction.

Any transaction which, based on the available information (provided by customer or from other source), reasonably appears not to be from a legitimate source or appears to be used for money laundering & financing of terrorism shall be refused.

Reports of suspicious transactions, or proposed transactions, shall be furnished, through the appropriate internal channels and, where required by regulatory guidelines, to the relevant external authorities.

Full cooperation shall be extended for any lawful request made by government agencies during their investigations into money laundering without “tipping-off” the customer.

No information of customer collected through CDD shall be provided or disclosed in any type of conditions by any ways to none, except to the agency, organization or official legally mandated to receive such information.

Detailed procedure for reporting of suspicious transactions shall be as described in the **Procedural Guidelines framed under this Policy.**

There shall be clear documented procedurals in place to enable any member of staff to report knowledge or suspicion of money laundering as soon as possible. The process must include appropriate procedures to allow for the escalation of reports to senior management, and where appropriate, disclosure to external authorities.

Internal reporting procedures may allow for staff to consult with line management, who may wish to comment on any proposed report before escalating a report to the management. However, the procedures must allow all staff to make a report directly to the management.

Copies of disclosures made to the authorities must be retained, together with a record of any enquires undertaken to support the report. Similarly a record of the reasons for non-disclosure to the authorities of any internal reports must be retained to demonstrate that at the time there was insufficient suspicion to justify making such a disclosure.

Following the making of a disclosure, full and prompt co-operative must be given to all legal requests to provide further information to the authorities to assist their investigations into money laundering.

Under no circumstances should a customer be informed that a disclosure has been made, as such notification could prejudice an existing or potential investigation by the authorities.

Where, following a disclosure, the authorities allow the relationship to continue and management decisions to retain the account, subsequent activity must be subject to particularly close vigilance. Any new activity that adds to the original suspicion must be disclosed.

7.8 Training and Awareness

Awareness on prevention of money laundering & financing of terrorism shall be raised through a periodic and regular training to all the staff members of the bank about what money laundering & financing of terrorism is, the recognition of suspicious transactions, the regulatory requirements on prevention of money laundering and financing of terrorism, Bank's policy, procedure and controls for prevention of money laundering & financing of terrorism. The trainings shall be accompanied with a Skill Assessment Test on AML/CFT awareness. A separate Procedural Guidelines shall be developed for effective management of trainings and skill assessment test on AML/CFT.

There shall be necessary arrangements in place to provide training on prevention of money laundering & financing of terrorism and other relevant issues to all of its related employees.

AML Implementing Officer shall ensure that arrangements in place to provide training on money laundering prevention and other relevant issues are adequate and effective.

AML Implementing Officer shall also ensure that periodic, more job specific, training is provided to relevant staff who is directly involved in account opening, transaction processing and establishing new customer relationships.

The Compliance Unit shall retain the documentary evidence of the trainings conducted with details (date of training, name & job of staff receiving the training and topics/issues covered/discussed in the training). **The documentary evidence of the training conducted shall be retained as prescribed.**

7.9 Independent Testing

The AML/CFT framework of the Bank shall be tested and reviewed by independent function such as internal audit, statutory audit, external auditors etc. Such testing shall be conducted at least once every year.

8. Record Retention

- Customer's related information and details shall be obtained regularly. The documents, data and information obtained under CDD shall be reviewed and kept as prescribed.

- Procedures/Guidelines shall be established to retain adequate records of identification, address verification, account opening, and transactions for a prescribed period. Identification and account opening records must be retained for a prescribed period after a relationship has ended. Records relating to internal and external suspicious transaction reports should also be retained for a prescribed period.

- All the documents pertaining to the prevention of Money Laundering and Combating Financing of Terrorism shall be retained for the period as prescribed by the law of the land.

9. Code of conduct of employees

Employees are also the customers of the Bank. All the employees shall be continuously trained and informed about the mechanism being developed regarding the control of Anti Money Laundering and financing of terrorism and methods and trends being used in money laundering, responsibilities to implement the laws pertaining to money laundering and financing of terrorism, know your customers and reporting of suspicious transactions. While recruiting/hiring the employees, due care shall be taken regarding the AML issues.

The employees filing the suspicious report must not Tip Off. He/she needs to maintain following code of conduct. He/she:

- Must not inform/warn the customer about the suspicion,
- Must not talk/disclose with other employees and friends/family,
- Must comply with the instructions of the competent authority and the department head whom he/she had reported, and
- Must assist and cooperate with the competent authorities in investigation.

The code of conduct has two aspects:

- The relationship with the customer will not be damaged if the authorities regard the account transaction as bona fide and,
- If the customer/transaction found to be act of money laundering, the authority will be in a better position to catch the blueprint and there will be less chance of eroding the evidence.

Employee failing to report suspicious and unusual transaction shall attract legal and disciplinary action.

10. Speaking Up

There shall be a speaking up mechanism instigated in the Bank such that any staff member who suspects that the Bank's code of conduct, prudent practice, and ethical standard is being/has been compromised contemplating or facilitating any act of Money Laundering /Terrorist Financing are allowed to escalate the case to senior management. The management shall provide adequate safeguards against victimization of whistle blower including the anonymity of the whistle blower.

11. Risk Appetite and Tolerance

The Bank shall pursue a zero tolerance policy on all matters related to AML/CFT compliance.

12. Enforcement and Effective Discharge of Roles & Responsibilities

There shall be clear lines of internal accountability, responsibility and internal/external reporting in connection with prevention of money laundering & financing of terrorism. The primary responsibility of prevention of money laundering rests with the Business Units/Branches which must ensure that appropriate internal controls are in place and are operating effectively and that staffs are adequately trained. The business Units and Branches shall be supported in meeting their responsibilities by the relevant departments/ units including Compliance, Operation and Legal Department.

12.1 Roles & Responsibilities of the Board of Directors

The Board of Directors shall be responsible for reviewing/approving this policy document on prevention of money laundering & financing of terrorism. As per the NRB Directives/Circulars, the Board shall review the status of implementation of Anti Money Laundering Act, 2064, Anti Money Laundering Rules, 2066, and the provisions contained in the Directives/Circulars issued by NRB related to AML/CFT at least on quarterly basis and furnish the review report on the implementation of the directives to FIU on half yearly basis. As per the AML Directives to the Banks & Financial Institutions, the Board of Directors of the bank and financial institutions shall, at least on quarterly basis, discuss on setting up and improving mechanisms to prevent customer's suspicious and abnormal transaction or money laundering and make necessary arrangement for this effect.

Hence, the Board of Directors of the Bank shall effectively discharge its statutory responsibilities as elaborated hereinabove.

12.2 Roles & Responsibilities of the Chief Executive Officer

The Chief Executive Officer shall be responsible for reviewing/approving the control, monitoring and reporting procedures on prevention of money laundering & financing of terrorism that meet standards set by this policy documents. The Chief Executive Officer shall also be responsible for approval of all required procedural guidelines based on the policies set by this document.

Directive No. 9(3) of the FIU Directives to Banks and Financial Institutions states that "It shall be responsibility of the Chief Executive Officer of the Concerned bank and financial institutions to review on quarterly basis as to whether or not the provisions of Anti-Money Laundering Act, and rules, directive, order or policy formulated under such act are complied with and submit a report to Financial Information Unit completing the review of the same in three month from the end of fiscal year. Further, a brief summary relating to this shall also be disclosed in the annual report of the institution."

12.3 Roles & Responsibilities of the Chief Operating Officer

The Chief Operating Officer shall be responsible for ensuring proper implementation of checks and control and monitoring and reporting procedures across the Bank.

12.4 Roles & Responsibilities of Unit Heads

Unit Heads shall be responsible for ensuring proper implementation of control and monitoring and reporting procedure across the unit under their control

12.5 Roles & Responsibilities of Operation Managers

Operation Managers shall be responsible for ensuring proper implementation of control, and monitoring and reporting procedure across the branch under their control.

12.6 Roles & Responsibilities of Internal Auditor

Internal Auditor shall be responsible for conducting checks and reviews to ensure that the control and monitoring and reporting procedures under this policy and the policy itself are properly followed across the Bank.

12.7 Roles & Responsibilities of Branch KYC and AML/CFT Implementing Officer

Branch KYC and AML/CFT Implementing Officer shall be responsible for ensuring implementation of this Policy and Procedures & Guideline framed hereunder, review of high value and high risk transaction, and report suspicious transactions/ activity under the guidance of Chief Operating Officer and AML Implementing Officer of the Bank. The roles and responsibilities shall be as assigned in the letter to designate the Branch KYC and AML/CFT Implementing Officer.

Chapter-III: Miscellaneous

13. Amendment and Interpretation

This policy shall be reviewed annually. In case any confusion in the interpretation of this policy arises, the matter shall be referred to the Board of Directors through CEO and the decision made by it shall be the final and binding.

14. Consistency with Laws & Changes in Law/ Rules/ Regulations/ Directives/ Guidelines

This policy must be read in conjunction with the prevailing laws of land pertaining to AML/CFT such as Anti Money Laundering Act, 2064; Anti Money Laundering Rules, 2066; Suspicious Transactions Reporting Guidelines and Threshold Transactions Reporting Guidelines issued by FIU; the guidelines/directives issued by the NRB and all other related acts/guidelines issued by other regulatory authorities from time to time.

In case there happens to be any contradiction with the prevailing laws currently in effect or the laws that introduced in future, the subject matters contained in this policy shall be *ab initio* void to the extent of contradiction

15. Power to Formulate Appropriate Manuals/Guidelines

The CEO is authorized to approve appropriate Manuals/Guidelines required for the effective implementation of the provisions contained in this policy. Such Manuals/Guidelines shall be construed as the part of this policy and shall be read in conjunction with the provisions contained in this policy. There shall not be any contradiction in the Manuals/ Guidelines with this policy and any contradiction in the Manuals/Guidelines with this Policy shall be *ab initio* void to the extent of contradiction. The Manual/Guidelines shall be approved by the CEO and the same shall be furnished to the Board for information.

16. Retrospective Application

The standards set by this policy document apply to both new and existing business relationships. It is therefore necessary to initiate corrective actions on customer identification and customer due diligence, where required, for the existing accounts no matter how long the relationship has been in operation. Where significant numbers of accounts are involved, work plans for corrective actions should prioritize relationships representing higher risk.

17. Repeal & Saving

This Policy shall supersede the Bank's Policy for Prevention of Money Laundering & Combating Financing of Terrorism approved by the Board of Directors for implementation on September, 2014. Any acts done actions taken under the Policy shall be deemed to have been done and taken under this policy