एन आई सी एशिया बैंक लि.

NIC ASIA Bank Limited

Policy for Prevention of Money Laundering and Combating the Financing of Terrorism 2017

NIC ASIA Bank Limited

Policy for Prevention of Money Laundering and Combating the Financing of Terrorism 2017

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- 2017" vide its 297th Board Meeting dated 13/04/2017 for implementation after review and recommendation of 87th meeting dated 30/03/2017 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
4	4th	Board of Directors	April 13, 2017

NIC ASIA
एन आई सी एशिया बैंक लि.

Approval Sheet

Recommended By	Ramesh Prasad Joshi Head-Compliance Department	(Original Signed)
Reviewed & Supported By	Roshan Kumar Neupane Chief Risk Officer	(Original Signed)
Reviewed By	Dipak Dhakal Head Internal Audit	(Original Signed)
Reviewed By	Laxman Chalise Manager-Retail Loans Department	(Original Signed)
Reviewed By	Bishal Sigdel Manager- Finance	(Original Signed)
Reviewed By	Sushil Bhattarai Manager – IT	(Original Signed)
Reviewed By	Parmeswor Shrestha Head Digital Banking	(Original Signed)
Reviewed By	Dipendra Rajbhandari Head CAD	(Original Signed)
Reviewed By	Rajesh Rawal Deputy Chief Operating Officer	(Original Signed)
Reviewed By	Dinesh Bhari Head Legal and Corporate Affairs	(Original Signed)
Reviewed By	Shilu Aryal Head-Deposit & Transaction Banking	(Original Signed)
Reviewed By	Jayendra Rawal Head-Corporate Loan and Projects Financing	(Original Signed)
Reviewed By	Sudhir Pandey Chief Operating Officer and Head HR	On Leave
Supported By	Laxman Risal Chief Executive Officer	(Original Signed)

NIC ASIA
एनआईसी एसीया बैंक लि.

Contents

Abbreviations

ALPA	Assets (Money) Laundering Prevention Act, 2008
AML	Anti Money Laundering
APG	Asia Pacific Group on Money Laundering
BCBS	Basel Committee for Banking Supervision
CAP	Customer Acceptance Policy
CBS	Core Banking Software
CDD	Customer Due Diligence
CFT	Combating Financing Terrorism
DNFBPs	Designated non-financial Businesses and Professions
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Information Unit
KYC	Know Your Customer
ML	Money Laundering
NRB	Nepal Rastra Bank
PEP	Politically Exposed Person
PIP	Person in Influential Position
SOP	Standard Operating Procedures
STR	Suspicious Transaction Report
TTR	Threshold Transaction Report

NIC ASIA
एन आई सी एशिया बैंक लि.

Chapter 1

Introduction, Short Title and Commencement

1.1 Introduction, 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 (hereinafter referred to as the "Board") has approved this policy. This policy has laid down appropriate framework for effective compliance to prevailing Asset (Money) Laundering Prevention Act 2064 (second amendment), Anti (Money) Laundering Prevention Rules 2073, and Directives issued by Financial Information Unit (FIU) and Nepal Rastra Bank (NRB) from time to time

Name of Policy Document	**:**	**Policy for Prevention of Money Laundering & Combating Financing of Terrorism 2017**
Ownership	**:**	**Compliance Department**

This Policy shall be known as the "Policy for Prevention of Money Laundering & Combating Financing of Terrorism 2017" and shall came into force from the date of approval of the Board.

1.2 Terms and their Definitions

Unless otherwise specifically indicated, the following terms used in the ***"Policy for Prevention of Money Laundering and Combating the Financing of Terrorism-2017"*** shall have the following meaning(s):

a. "**The Bank**" means NIC ASIA Bank.
b. "**The Board**" means Board of Directors of NIC ASIA Bank.
c. "**Chairman**" means the Chairman of the Board of Directors of NIC ASIA Bank.
d. "**Chief Executive Officer / (CEO)**" means person appointed as The Chief Executive of the Bank, appointed by the Board and entrusted with overall Management, Administration and Operations of the Bank and accountable to the Board.
e. "**Chief Operating Officer /(COO)**" means the Officer or such designated official having other titles of the Bank, who shall be responsible for overall Operations of the Bank.
f. "**Unit Head**" refers to heads representing business unit or support unit and may be Head of Business Banks or Head of Consumer Banking or Head of Treasury (HT) or Head of Operation or Head of Retail Banking or Head of Credit or such Unit Heads as designated by CEO from time to time.
g. "**Branch Managers**" means heads of branches of the Bank.
h. "**Department Head**" means the head of a particular department of the Bank.
i. "**Competent Authority**" in relation to the exercise of any power means the Board, committee under Board, CEO, Head of Operations, Business Unit Heads, Branch Managers, Unit Heads, Department Heads or any other authority to whom such power is delegated by the Board or CEO from time to time.
j. "**RMC**" refers to the Board level Risk Management Committee of the Bank.
k. "**The Policy**" refers to "Policy for Prevention of Money Laundering and Combating the Financing of Terrorism-2017"

I. Money Laundering (ML):

Money laundering refers to any of the following acts:

1. The conversion or transfer of funds, by any person who knows, should have known or suspects that such funds are the proceeds of crime, for the purpose of concealing or disguising the illicit origin of such funds or of assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his actions.

2. The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to funds by any person who knows, should have known or suspects that such funds are the proceeds of crime.
3. The possession, acquisition, or use of funds by any person who knows, should have known or suspects that such funds are the proceeds of crime.

m. Financing Terrorism

An act committed by any person who, in any manner, directly or indirectly, and willingly, provides or collects funds, support, or attempts to do so, in order to use them or knowing that these funds will be used in whole or in part for the execution of a terrorist act, or by a terrorist or terrorist organization.

n. "Act", "Rules" and "Directive"

In this policy, "Act" will refer to the Asset (Money) Laundering Prevention Act 2064 and its latest amendment. The "rules" will refer to the Asset (Money) Laundering Prevention Rules 2066 and 2073 and "Directive" will refer to the directive issued from Nepal Rastra Bank and Financial Information Unit.

o. Terrorist

Any natural person or organization who commits the following acts:

1. Commits or attempts to commit terrorist acts by any means, directly or indirectly, unlawfully and willfully,
2. Participates as an accomplice in terrorist acts,
3. Organizes or directs others to commit terrorist acts, or
4. Contributes or cooperates to the group of persons acting with a common purpose of commission of terrorist acts where such contribution or cooperation is made intentionally and with the aim of furthering the terrorist act or with the knowledge or the intention of the group to commit a terrorist act.

NIC ASIA
एन आई सी एशिया बैंक लि.

p. Corresponding Banking

The provision of banking services by one financial institution (correspondent bank) to the customer of another financial institution (respondent bank).

q. Proceeds of crime

Any property derived from or obtained directly or indirectly through the commission of money laundering or predicate offence and it shall also include any other property and economic advantage gained or derived from such property or any property transferred or converted into other property or advantage, in full or in part, from such property or advantage.

r. Transaction

Any agreement made in order to carry out any economic or business activities and the term also means the purchase, sale, distribution, transfer or investment and possession of any assets, or any other acts as follows:-

1. Establishing business relationship,
2. Opening of an account,
3. Any deposit or collection, withdrawal, exchange or transfer of funds in any currency or instruments, payment order by electronic or any other means,
4. Use of any type of safe deposit box (locker),
5. Entering/establishing into any fiduciary relationship,
6. Any payment made or received in satisfaction, in whole or in part, of any contractual or other legal obligation,
7. Any payment made or received in respect of a lottery, bet or other game of chance,
8. Establishing or creating a legal person or legal arrangement, or
9. Such other act as may be designated by the Government of Nepal by publishing a notice in the Nepal Gazette.

s. Legal Person

Any company, corporation, proprietorship, partnership firm, cooperatives, or any other body corporate

NIC ASIA
एन आई सी एशिया बैंक लि.

t. Legal Arrangement

Trust (express trust) or other similar kind of legal arrangements

u. Client/ Customer

Any individual or entity who seeks/attempts to enter or has already entered into a business relationship, or conducts a one-off transaction with the bank as principal or as an client agent. Any person or entity connected with a financial transaction that may impose significant reputational or other risks to the Bank.

v. Employee / Staff

Employee / Staff means employee / staff of the Bank as defined in the Staff Service Bylaws of the Bank.

w. Domestic Politically Exposed Persons (PEP)

The President, Vice-President, Minister, parliamentarians, officials of the constitutional bodies, officials remained in the special class or equal to special class or their senior of the Government of Nepal, judge of the Appellate Court and their senior, senior politician, central member of national political party or senior executives of any institution partially or fully owned by the Government. It shall also include other group of person as designated by the Government of Nepal upon the recommendation of National Coordination Committee.

x. Foreign politically exposed person

Politically exposed person who is or has been the Heads of State or of government, senior politician, central member of national political party, senior government, judicial or military official, senior executives of state owned corporations of a foreign country.

y. Beneficial owner

Natural person who, directly or indirectly, owns or controls or directs or influences a customer, an account, or the person on whose behalf a transaction is conducted, or exercises effective control over a legal person or legal arrangement or remains as an ultimate beneficiary or owner of such activities.

z. Customer Due Diligence (CDD)

Customer Due Diligence is the process of identifying and evaluating the customers and the assessment of customer risk as part of know your customer (KYC) process, allowing banks to better identify, manage, and mitigate the AML related risks. The level of due diligence is based on the risk level of the customer and thus there may be various levels of due diligence prescribed by the regulators or decided by the bank. Currently, following are the categories of due diligence specified in NRB directive:

i. Standard/Normal Customer Due Diligence

This is conducted for low risk customers who do not fall under enhanced and simplified customer due diligence.

ii. Simplified Customer Due Diligence (SCDD)

This can be conducted for customers who fall under low risk customers having characteristics as specified by NRB directive i.e. whose total annual deposit or transactions remain within the limit of NPR 500,000, financial institutions supervised by NRB, customers whose identity is publically available and controlled by national system and other specified by regulator from time to time.

iii. Enhanced Customer Due Diligence (ECDD)

Enhanced Customer Due Diligence is conducted for high risk and medium risk customers. It refers to the additional due diligence pertaining to the identity of the customer, source of income, nature and value of transaction and others specified by directives.

aa. Risk Based Approach (RBA)

The approach of management which focuses on identifying and addressing potential risks of money laundering and terrorism financing. The core of this approach is to creating the match between “risks and controls” by understanding of the ML/TF risks to which the banks are exposed and apply AML/CFT measures in a manner and to an extent which would ensure mitigation of these risks. There is no universally accepted

methodology, which prescribe nature and extent of risk based approach. It provides every bank the flexibility to manage their ML/FT risks in their own way.

bb. Suspicious Transaction:

A transaction, including an attempted transaction, whether or not made in cash, which to a person acting in good faith;

- Gives rise to a reasonable ground of suspicious that it may involve proceeds of an offenses specified in law and regulations, regardless of the value involve.
- Seeks to conceal or disguise the nature or origin of funds derived from illegal activities
- Appears to have no economic rationale or bona-fide purpose
- Appears to be in circumstances of unusual, or unjustified complexity
- Appears to be deviated from profile, character and financial status
- Seems to be made with the purpose of evading the legal and regulatory reporting requirements
- Found to be conducted to support the activities relating to terrorism

cc. Suspicious Transaction Report:

A report to be made by Financial Institutions to Final Information Unit on any suspicious transactions or any attempts under the provisions of "Pariched 3, 7dha- Asset (Money) laundering prevention Act 2064" and point no. 19 of NRB Directive no. 19.

NIC ASIA
एन आई सी एशिया बैंक लि.

dd. Wire Transfer:

Any transaction carried out on behalf of an originator (both natural persons and legal entities) through the bank by electronic means with a view to making an amount of money available to a beneficiary person at another FI. The originator and the beneficiary may be the same person.

ee. 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.

ff. Shell Bank/entity

A bank or entity, which has no physical presence in the country in which it is incorporated, licensed or located, and which is not affiliated with a regulated financial services group that is subject to effective consolidated supervision. For the purpose of this clause, presence of local agent or junior level staff does not constitute physical presence. Shell banks/entities 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.

gg. 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 or by with whom such purchases is made by the Bank.

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, and NRB Directive wherever relevant.

1.3 Scope and Applicability:

This policy shall be applicable to all the staffs, Bank functions and structures. If any department, branch or business unit of the Bank is unable, in an exceptional circumstance, to apply the standards set by this policy, they must have pre-facto approval of the Chief Executive Officer (CEO) in recommendation of the Chief Operating Officer, Chief Risk Officer, and AML implementing Officer.

1.4 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 broad framework for formulation and implementation of various manuals or procedural guidelines that is required for effective AML/CFT & KYC compliance.

1.5 Money Laundering and Financing of Terrorism

a. 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 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".

b. 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.

एन आई सी एशिया बैंक लि.

c. Money Laundering Process

The Money Laundering consists of the following processes:

- **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.

- **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.

- **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.

d. 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.

e. Risks of money laundering and terrorist financing to the banks

Bank is exposed to several risks if it fails to prevent the Bank being used for M/L and F/T activities.

- **Reputational risk:** The reputation of a business is usually at the core of its success. The ability to attract good employees, customers, funding and business is dependent on reputation. Even if a business is otherwise doing all the right things, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong AML/CDD/CFT policy helps to prevent a business from being used as a vehicle for illegal activities.

- **Operational risk:** This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If AML/CDD/CFT policy is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound.

- **Compliance Risk:** Risk of loss due to failure of compliance with key regulations governing the Bank's operations.

- **Legal risk:** Risk of loss due to any of the above risk or combination thereof resulting into the failure to comply with Law and having a negative legal impact on the Bank. The specific types of negative legal impacts could arise by way of fines, confiscation of illegal proceeds, criminal liability etc.

- **Financial risk:** Risk of loss due to any of the above risks or combination thereof resulting into the negative financial impact on the Bank.

f. International Initiatives

The international community has acted on many fronts to respond to the growing complexity and the international nature of rapidly evolving ML/FT methods. The emphasis is on promoting international cooperation and establishing a coordinated and effective international AML/CFT regime. Many international agencies have helped countries develop a capacity to prevent and counter ML. The following presents some of the main elements of the global and regional initiatives.

- The Financial Action Task Force (FATF) was established in 1989 by the G-7 countries to respond more effectively to ML. The FATF Forty Recommendations require the criminalization of ML. In addition, the recommendations call on countries to adopt legislative and other measures in order to: freeze, seize and confiscate criminal proceeds; waive bank secrecy laws to permit financial institutions to monitor and report suspicious transactions; protect those reporting these transactions from civil and criminal liability; establish financial investigation units; and, cooperate fully in international law enforcement efforts to combat ML. The FATF Special Recommendations require countries to criminalize the financing of terrorism, terrorist organizations and terrorist acts and to designate these new offences as ML predicate offences. The FATF is also involved in monitoring the progress of members in complying with its recommendations.

- The United Nations Convention on Illicit Trafficking in Narcotic Drugs and Psychotropic Substances (Vienna Convention), the UN Convention against Transnational Organized Crime (Palermo Convention), the UN Convention against Corruption and the International Convention for the Suppression of the Financing of Terrorism all contain provisions relating to the tracing, freezing, seizing and confiscation of instrumentalities and proceeds of crime.

- Financial regulation standards are also set by the Basel Committee on Banking Supervision. In 1988, the Basel Committee put forward some basic principles as part of its Statement for the Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering. It has also issued a paper a "sound management of risks related to money laundering and financing of terrorism in 2014".

- Wolfsberg Group, which is non- governmental organization of 13 large commercial banks founded in AD 2000, develop and publishes financial industry standards for Anti-money laundering (AML), Know Your Customer (KYC) and Counter Terrorist Financing (CTF) policies. Its work is similar to what the Financial Action Task Force on Money Laundering (FATF) does on a government level.

- Many countries have established financial intelligence units (FIUs) as a focal point for the AML efforts and a point at which information is exchanged between financial institutions and law enforcement. Since 1995, a number of these units have begun to work closely together, to exchange information and to coordinate their AML efforts. They formed the Egmont Group which facilitates international exchanges and cooperation among FIUs in relation to both ML and FT.

- Multi-lateral organizations like World Bank, International Monetary Fund, Asian Development Bank also work on preventing ML/FT risks. They also provide financial and technical assistance to countries wishing to implement the FATF 40+9 recommendations. They have also published several papers on the theme of preventing ML/FT risks for the financial industry.

- As part of its work to promote good governance and to fight corruption, the Commonwealth has long been involved in international AML/CFT efforts. In 1993, it made available a Commonwealth Model Law. In 1996, it developed Guidance Notes for the Financial Sector which was revised in 2000 and in 2005 based on best practices.
- Asia Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organization founded in 1997 in Bangkok, Thailand consisting of 41 members. APG members are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism. Nepal became the member of APG Group in June 2002.

NIC ASIA
एन आई सी एशिया बैंक लि.

Chapter 2

Legal and Regulatory Obligations and International Standards to be followed

The bank is obliged to comply with the requirements of the following laws, rules and regulations of the homeland. In addition, Nepal has to follow standards prescribed by FATF as an obligation of member country of Asia Pacific Group on Money Laundering, which is a FATF style regional body.

2.1 Legal Obligations:

The bank is obligated to comply with the requirements of the following Laws and rules:

a. Asset (Money) Laundering Prevention Act, 2064 (Including second amendment)
b. Asset (Money) Laundering Prevention Rules, 2073:

2.2 Regulatory Obligations:

a. Unified Directives No. 19 issued by Nepal Rastra Bank:
b. Directives issued by FIU to implement United Nations Security Council's Resolutions 1267 & 1373)
c. Anti-Money Laundering Directives to Bank & Financial Institutions issued on 2066 Bhadra 1
d. Directive no. 2 on suspicious transactions issued by FIU on 2066 Chaitra (this directive repealed earlier directive no. 1)
e. Guidelines for Detecting Suspicious Transactions issued by FIU effective from 15th January 2014
f. Guidelines for Threshold Transactions Reporting issued by FIU effective from 15th January 2014

2.3 Major Contents of Anti Money Laundering Act 2064 relevant to the banking sector

Chapter 1: Preliminary (Short Title, Extent and commencement and Definition of terms)

Chapter 2: Money Laundering and Terrorist Financing offences

Not to launder property

Not to commit offense of terrorist financing

Act committed in foreign state to be an offense

Chapter 3: Provisions on Customer Identification and Transaction

- Prohibition on anonymous or fictitious accounts
- Prohibition against shell bank
- Customer Identification to be required
- Special provision for identification of politically exposed persons
- Beneficial ownership to be identified
- Risk Assessment and management
- Enhanced CDD
- Simplified CDD
- CDD of existing customer
- Timing of identification
- Ongoing Monitoring
- Identification and verification by Third party
- New Technology and non-face to face customer or transactions
- Obligations regarding wire Transfers
- Provision on Cross Boarder Correspondent Banking
- Special Monitoring of Certain Transactions
- Not to carry out transactions
- Responsibilities of Reporting Entities
- Compliance with obligations by foreign subsidiaries and branches
- Record Keeping
- Obligation to report suspicious transactions

2.4 Major Contents of Anti Money Laundering Rules 2073 relevant to the banking System

Chapter 1: Preliminary (Short Title, Extent and commencement and Definition of terms)

Chapter 2: Provisions on Reporting Entity

- Customer Identification and Transactions

- Customer Identification for occasional transactions
- Minimum information/documents to be taken for customer identification
- Document verification for customer identification
- Identification of beneficial owner/s
- Enhanced due diligence
- Simplified Customer Due Diligence
- Non Face to Face customers or transactions
- Prohibited Transactions
- Record retention
- Limitation on Transaction
- Report submission using electronic mediums

2.5 Major Contents of NRB directive 19 which is fully relevant to the bank

1. Policy, procedures and practices
2. Risk Based Customer Identification Procedure
3. Customer Identification
4. Identification of Beneficial Owner
5. Acceptable delay in verification of customer identity in exceptional situation
6. Risk identification, assessment and risk profiling
7. Use of Third Party
8. Acceptance of new customer
9. Continuous maintenance of customer's information
10. Continuous monitoring of customer's transactions
11. Termination or relationship with the customer
12. Enhanced due diligence for high risk customers
13. Simplified due diligence for designated categories of low risk customers (small depositors having annual transactions of less than NPR 500,000)
14. Policies and procedure regarding wire transfer
15. Policies regarding correspondent banking
16. Safe keeping of records
17. Reporting of threshold transactions

18. Exemption in reporting requirement of TTR for specific categories of customers
19. Submission of STR to FIU
20. Restriction in providing information to unauthorized persons and protection of employees for reporting made with good intention
21. Internal policies, procedures, systems and Controls
22. Implementing policies and procedure to prevent misuse of technology
23. Provisions regarding shell bank
24. Implementing instructions of home ministry regarding blocking accounts/assets of terrorists decided and listed by UN Security council.
25. AML/CFT reporting as required by Bank Supervision department using an official web page of NRB

2.6 Major contents of Directive issued by FIU

1. Customers to be clearly identified and records thereof maintained
2. Particulars to be provided by customers
3. Particulars regarding transactions of threshold amount or in excess of such threshold to be submitted
4. Exemption from reporting obligations
5. Statement of suspicious transactions to be submitted
6. Classification and mitigation of risk
7. Compliance officer
8. Responsibility of compliance officer
9. Responsibility of bank and financial institutions
10. Procedure of filing particulars
11. Internal directives
12. Information and training
13. Monitoring and regulation
14. Maintenance of secrecy
15. Penalty and Actions

NIC ASIA
एन आई सी एशिया बैंक लि.

2.7 Major Contents of Directive on Suspicious Transaction issued by FIU (including addition)

1. Nature of functions those require reporting as suspicious to FIU
2. Terrorist Identification, restriction in transaction and reporting to FIU
3. Additional reasons or basis for reporting as suspicious activity or transaction
4. Risk Classification
5. Risk identification
6. Submission of report of international wire transfers
7. Action, fine & penalty and punishment

2.8 International Standards (FATF Recommendations)

Being the member country of Asia Pacific Group on Money Laundering, Nepal has to implement FATF recommendations as required or applicable. FATF introduced forty recommendations in 1990, for the first time, as an initiative to combat money laundering and terrorist financing risks. In 1996 the recommendations were revised to reflect evolving money laundering typologies. These recommendations have been endorsed by more than 130 countries and are being applied by countries in varying extent as the international anti-money laundering standard. FATF reviews recommendations from time to time and publish recommendations with changes or enrichment. The latest publication of recommendations by FATF is on 2012. These recommendations have provided an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing throughout the world. The FATF recognizes that countries have diverse legal and financial systems and so all cannot implement identical measures to achieve the common objectives, especially over matters of detail. The recommendations therefore set minimum standards for action for countries to implement the detail according to their particular circumstances and constitutional/legal 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 the international co-operation.

The major themes on which FATF recommendations have been issued on 2012 relating to money laundering are as follows:

1. Assessing risks & applying a risk-based approach
2. National cooperation and coordination
3. Money laundering offence
4. Confiscation and Provisional measures
5. Terrorist financing offence
6. Targeted financial sanctions related to terrorism & terrorist financing
7. Targeted financial sanctions related to proliferation
8. Non-profit organizations
9. Financial institution secrecy laws
10. Customer due diligence
11. Record Keeping
12. Politically exposed persons
13. Correspondent banking
14. Money or value transfer services
15. New technologies
16. Wire transfers
17. Reliance on third parties
18. Internal controls and foreign branches and subsidiaries
19. Higher-risk countries
20. Reporting of suspicious transactions
21. Tipping-off and confidentiality
22. DNFBPs: Customer due diligence
23. DNFBPs: Other measures
24. Transparency and beneficial ownership of legal persons
25. Transparency and beneficial ownership of legal arrangements
26. Regulation and supervision of financial institutions
27. Powers of supervisors
28. Regulation and Supervisions of DNFBPs
29. Financial intelligence units
30. Responsibilities of law enforcement and investigative authorities
31. Powers of law enforcement and investigate authorities
32. Cash couriers
33. Statistics

NIC ASIA
एन.आई.सी एशिया बैंक लि.

34. Guidance and feedback
35. Sanctions
36. Internal instruments
37. Mutual legal assistance
38. Mutual legal assistance: freezing and confiscation
39. Extradition
40. Other forms of international cooperation

2.9 Regulatory Actions, Sanctions and fines/penalties:

NRB may take any or all of the following actions or sanctions against the bank failing to comply with any provisions of the Act, Rules and Directive:

- to issue written reprimand warnings,
- to impose fines from one million to NRs fifty million to the bank
- to impose full or partial restriction on the business or transaction,
- to suspend the registration or permission or license,
- to revoke the permission or license or cancel the registration
- Other appropriate sanctions

2.10 Not to be Liable for Providing Information:

- No staff or official of the bank is supposed to have violated the professional or financial norms prescribed under other prevailing laws if such act has been carried out in the course of discharging duties under the Asset (Money) Laundering Prevention Act up to the level of performance mandated under the Act.
- No criminal, civil, disciplinary or administrative action or sanction shall be taken against the bank or any of their official or staff who in good faith submit reports or provide report, document, information, notice or records in accordance with the provisions of ALPA, rules and directives as a breach of secrecy provision under prevailing laws or contractual, administrative or regulatory liability.

Chapter 3

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

This policy represents the strategic orientation and management policies for preventing risks related to money laundering and terrorist financing chosen autonomously by the bank. This policy also has set expectations, standards and behaviors to prevent ML/FT risks for the bank. Following are the policies taken by the bank:

3.1 Full adherence to law and regulations

The bank is committed to full compliance with the money laundering laws and regulations applicable in the country.

3.2 Implementing evolving national and international best practices

The bank adopts policy of not only adhering country's legal and regulatory requirement, but also adopts international best practices to the extent reasonable and practicable to effectively manage ML/FT risks in the bank.

3.3 Use of Automated AML solution

It shall be the policy of the bank to make maximum use of technology and upgrade the systems and procedures in accordance with the upcoming challenges regarding ML/TF. Likewise, bank shall implement /use automated AML solutions across its network for effective KYC management, risk assessment, transaction monitoring etc.

3.4 Risk Appetite and Tolerance

The Bank shall pursue a zero tolerance policy on all matters related to AML/CFT compliance. The bank shall take action for resolving issues in high priority.

3.5 Customer Acceptance

The bank will not accept any person/entities as its customer if the customer and beneficial owner of the customer cannot be identified, verified and thus bank is unable to have customer's risk profiling as required by the Act, Rules and Directive

3.6 Risk Based Approach (RBA)

The RBA principals propose identification, assessment, understanding and mitigation of ML/TF risk including explicit consideration to key risk factors such as customers, products/services, transactions, geographic areas, and delivery channel and with varying degrees of impact and levels of risk. It is a continuous process, carried out with a dynamic approach.

The bank shall adopt Risk Based Approach (RBA) in managing its ML/FT risks and assess potential ML/FT risks and implement measures and controls commensurate with the identified risk. The bank shall strengthen, make priorities and perform its activities to manage higher risks first and ensure that greatest risks receive the highest attention. RBA shall be adopted in all activities that are performed to prevent ML/FT risks in the bank.

3.7 Risk Management via Three Lines of defense

For the effective assessment, understanding, management and mitigation of ML/FT risks, bank shall adopt three line of defense. Identification and analysis of ML/FT risks and effective implementation of policies and procedures to encounter the identified risk is the feature of effective and sound risk management. The line of defense shall act as safeguard of the bank during the adversities and shall be liable for effective risk management.

a. First line of defense:

Business units and departments shall function as a first line of defense to prevent ML/FT risks. Business shall promote AML/CFT principles while doing business. Businesses shall own and manage the ML/FT risks arising from the business. Persons involved in business functions must ensure that appropriate controls are in place and operating effectively. Business units shall make an appropriate risk assessment before introducing any product or service and implement required mitigations. It shall be the responsibility of compliance department to assist business units/departments in this process.

b. Second line of defense:

Compliance Department shall function as a second line of defense to prevent ML/FT risks in the bank. The Compliance Department shall monitor overall legal, regulatory and internal compliance of policies, procedures and guidelines. It shall also provide businesses with regulatory compliance expertise and guidance, set standards and trainings for businesses to manage and oversee ML/TF risks.

c. Third line of defense

This shall be performed by internal audit. The internal audit shall review the activities of the first two lines of defense with the purpose to ensure that legislation, regulations and internal policies are processed effectively.

3.8 Commitment of Senior Management

Senior management of the bank is fully committed to establishing appropriate policies, procedures and controls for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. Senior management also commits to ensure that ML/FT risks are understood and appropriately mitigated in the bank. It shall also ensure that effectiveness of controls shall be regularly reviewed. The senior management of the bank shall promote compliance as a core value and culture of the bank and the bank will not enter into, or maintain, business relationships that are associated with excessive ML/TF risks which cannot be mitigated effectively.

NIC ASIA
एन आई सी एशिया बैंक लि.

3.9 Prohibited customers and transactions:

It shall be the policy of the bank not to do the followings:

1. Establish or maintain anonymous accounts, or accounts in fictitious names or transact in such accounts or cause to do so.
2. Maintain relationship with shell Banks or other banks which deals with shell bank or shell entities
3. Establish an account or continue business relationship or conduct transaction with the customer who cannot provide documents, information and details required for the customer identification and verification as required by law and regulation. However, in

case customer submits valid reason for inability of presenting some document or information and bank become satisfied with the reason, relationship can be established and transaction can be done with maintaining record of the information of non-existence of document/information.

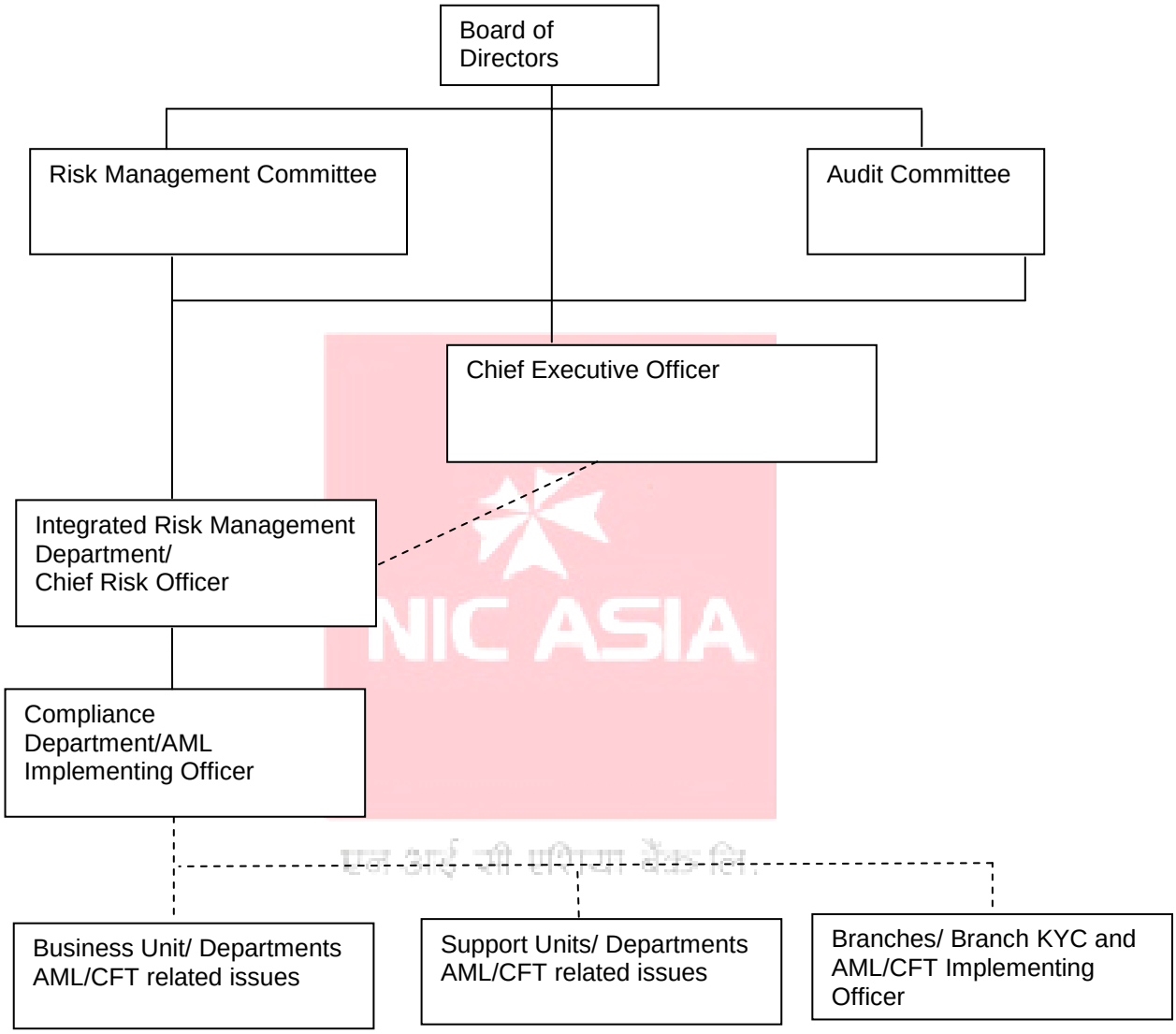
4. Customers who provide conflicting Documents, information and details.
5. Maintain relationship with the banks operating in offshore jurisdictions
6. Maintain relationship with persons and entities sanctioned by major sanction authorities such as United Nations, Office of Foreign Assets Control- United States, Her Majesty's Treasury-United Kingdom, etc.
7. Payment orders with an inaccurate representation of the person placing the order
8. Acceptance of payment remittances from other banks without indication of the name or account number of the beneficiary;
9. 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
10. Maintaining accounts under pseudonyms that are not readily identifiable
11. Opening Accounts without name or with notional name
12. Acceptances and documentation of collateral that do not corroborate with the actual economic situation or documentation of fictitious collateral for credit granted on trust
13. Payable through Accounts
14. Providing Downstream Correspondent Banking

NIC ASIA
एन आई सी एशिया बैंक लि.

3.10 Governance, Oversight, Structure and Reporting

In order to perform effective management of ML/FT risks, the board and senior management of the bank shall provide governance and oversight of the adequacy and effectiveness of management of ML/FT risks. They will also ensure that AML/CFT programs are aligned with relevant legal and regulatory requirement and AML/CFT strategy is optimally aligned with international best practices.

The AML/CFT management of the bank shall be carried out on the structure as depicted in following Organ gram



a. Compliance Department

The Bank shall have a Compliance Department under the purview of Chief Risk Officer which will look after the overall compliance of AML/CFT policies and procedures.

b. Appointment of AML Implementing Officer

The Bank shall appoint AML Implementing officer to function as a focal point for implementation of this policy, and guidelines formulated to execute 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.

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 AML/CFT related responsibilities. 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 11 of the Anti-Money Laundering Rules 2073 are as follows:

a) Function as focal point to perform tasks in accordance with the Act, Rules and the Directives,
b) Cause to maintain the secure record of the transactions,
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.

c. Branch KYC and AML/CFT Implementing Officer

For effective management of ML/FT risks in the bank, branch level KYC and AML/CFT implementing officer shall be appointed on each branch. Operation In charge / Operation Manager shall mandatorily be Branch KYC and AML/CFT Implementing Officer while the other staff of the branch may be appointed as alternate Branch KYC and AML/CFT Implementing Officer on the need basis. The Chief Executive Officer shall appoint upon the recommendation of AML Implementing Officer or Chief Risk Officer. 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 other functions, they shall report as per their job description.

3.11 Development and implementation of procedural guideline:

For the purpose of executing this policy, the bank shall develop and implement procedural guidelines on various functional areas 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 Department.

3.12 Know your Customer (KYC) and Customer Due Diligence

The Bank is aware that availability of sufficient customer information underpins all other AML procedures and should be seen as a critical element in the effective management of ML risks. The detail regarding customer acceptance shall be incorporated in specific guideline which lays down the criteria for the acceptance of customers. The guideline would form an integral part of the bank's AML Policy. The KYC procedures would be based on the following principles:

a. Customer Identification and verification

Customer Identification Process (CIP) is a critical part of the Customer Due Diligence process. It is essential to establish the true identity of the customers and be assured that the customers are not involved in any kind of money laundering and terrorist activities. Some of the key information that the bank requires to collect includes;

- Information regarding the family member's name
- Full customer identification 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 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.

b. Special Provisions for Identification of Politically Exposed Person (PEP):

The Bank shall establish a risk management system to identify whether a customer, person seeking to be customer or a beneficial owner of a customer or transaction is a

politically exposed person. It shall adopt the following additional measures if it finds the customer or beneficial owner is PEP:

- to obtain approval from senior management official while establishing a business relationship,
- to acquire approval from senior management official to continue the business relation with an existing customer if he is identified as a politically-exposed person
- to take all reasonable measures to identify the source of amount/fund and property of such customer or beneficial owner,
- to conduct ongoing monitoring of such customer and the business relationship,
- to apply Enhanced CDD measures

Provisions stipulated in sub-sections (1) and (2) shall be applicable to the family members and associated persons of foreign PEP, or international PEP or domestic PEP identified as high risk.

c. Beneficial Owners:

When establishing business relationship or conducting transaction with the customer, the bank shall identify the beneficial owner verify the identity of the beneficial owner taking reasonable measures to. Identification of beneficial owner shall be performed as per the procedural guideline framed under this policy.

NIC ASIA
एन आई सी एशिया बैंक लि.

d. KYC Risk Grading

The bank shall adopt three levels of KYC risk grading system in the bank. They are:

i. Low risk

ii. Medium risk

iii. High risk

All customer accounts and relationships shall be assigned a specific KYC risk grade. Risk grading shall be carried out as per the procedural guideline framed under this policy.

e. Risk based Customer Due Diligence

The bank shall follow risk based approach in conducting customer's due diligence as shown below:

i. Standard customer due diligence- for low risk customers

ii. Enhanced Customer due diligence- for medium and high risk customers

It shall be the policy of the bank not to adopt simplified due diligence unless it is made mandatory by the regulator.

f. Periodic review and update of Customer Due Diligence

The bank shall view CDD as an ongoing process and therefore, CDD information of the customers shall be regularly updated. The frequency of reviews and update shall be determined by the level of risk associated with the relationship. 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. Action 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.

g. Rejection or closure of customer relationship or transactions:

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.

3.13 Due diligence of Employees

Employees are also emerging as the great source of ML/FT risks for the bank. Therefore, the bank will arrange adequate screening mechanism as an integral part of recruitment/hiring process of staffs. The Human Resource Department of the bank shall conduct due diligence

of employees before appointing as staff and during service period. Due diligence of employees shall be performed as per procedural guideline framed under this policy.

3.14 Due Diligence of vendors, service providers, consultants and business partners

Vendors, service providers, business partners, consultants, etc. also can pose significant reputational risk to the bank if they are found involved in money laundering and terrorist activities and/or use the relationship for money laundering or terrorist activities. Therefore, the Bank shall not establish relationship with such parties if they are found involved in money laundering or terrorist financing before establishing a relationship. The bank shall conduct regular due diligence of these parties and additional risk management tools will be used, if risk is identified. Similarly, the bank shall report identified suspicious activities found to FIU as its regulatory liability. The execution of due diligence of such parties shall be done as per related procedural guideline.

3.15 Due diligence of correspondent banking relationships

Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Large international banks typically act as correspondents for several other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international transfers of funds, cheque clearing, payable-through-accounts and foreign exchange services. It would be the bank's policy to obtain sufficient information about correspondent banks to understand the nature of their business & activities. When considering entering into a cross-border correspondent banking relationship, the bank shall carry out due diligence measures i.e. ownership, Management Structure, major business activities, customers, purpose of the Account, location, etc. In addition, research will be conducted from publicly available information on the correspondent bank's business activities, their reputation, and quality of supervision and whether the institution has been subject to a money laundering or terrorist financing investigation or any regulatory action.

3.16 Recognition and reporting of suspicious activities and transactions:

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. 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 Detecting 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.

NIC ASIA
एन आई सी एशिया बैंक लि.

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.

3.17 Risk assessment

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 2073. 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 likely to encounter.

a. The bank shall identify and assess the money laundering or terrorist financing risks before launch of new product, service, business practice, use of new technology and initiating non-face to face customer services or transaction

b. The risk assessment shall include risks coming out from following sources:

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

c. While conducting risk assessment, the bank shall consider the findings of national and regulatory risk assessment.

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

e. The bank shall undertake customer due diligence measures in accordance with the level of risks as identified by risk assessment and shall establish appropriate policy,

procedural and risk management measures, to manage and mitigate such risks and update such measures.

3.18 Transaction and Account Surveillance

Effective ongoing monitoring is vital for understanding of customer's activities and is an integral part of effective AML/CFT system. It helps to know the customers and to detect unusual or suspicious activities. In line with the regulatory requirements, bank shall adopt the policy of monitoring the accounts in the mentioned time frame as per the risk category of the customer.

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 ML/FT threats.

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

Business 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.

3.19 Design and Implement Reviews, Checks and Control:

The Bank shall have adequate procedures and processes to ensure effective checks, reviews and controls in executing AML/CFT and KYC Compliance. Such reviews, checks and controls shall be designed to help the businesses meet their responsibilities in relation to the prevention of money laundering & financing of terrorism. These standards shall be primarily based on the relevant regulatory/statutory guidelines and the best practices on prevention of money laundering. These checks, reviews and controls shall be regularly updated to identify and mitigate continuously evolving risks. The Bank shall implement checks, reviews, controls in all its functions, products/services, processes, etc. The operating manuals, product paper guidelines, procedural guidelines, standard operating procedures, etc. shall incorporate related checks and controls.

3.20 Sanction Screening

The Bank shall not establish any kind of relationship (customer, employee, vendor, consultant, service provider, business partner, etc.) with sanctioned individuals/entities listed in the Sanction List published by UN, OFAC, HMT-UK etc. Sanction screening shall be the integral part of due diligence process and thus the sanction screening shall be conducted while updating identity and conducing further due diligence. The banks shall also conduct sanction screening of individuals and entities other than primary/main customers/relationship holders who are linked in any manner with customer/ primary relationship holder and bank believes that it can face risk due to those persons and entities. The bank shall decide about such associated persons/entities whose screening will be performed. The screening function shall be performed as per related guideline framed under this policy.

3.21 Employee Education and Training programs

a. Compliance with Statutory and regulatory requirement:

The bank is responsible to fully comply the entire statutory and regulatory requirement relating to training and awareness of the employees.

b. Risk Based Approach in conducting training and awareness program

The bank shall adopt a risk based approach while conducting training programs. The bank shall aim, strengthen, priorities, and conduct trainings in line with the result of bank's risk assessment as well as emerging ML/FT risks identified by the bank.

c. Education and Training programs

The bank shall conduct educational and training programs relating to ML/FT risks and their management as its regular activity. It shall be the bank's policy to provide basic awareness training to all the staffs and other job/responsibility specific trainings on core risk functions/areas i.e. trade finance, credit, customer service, compliance, etc. Such programs may include seminars, workshops, discussions, trainings etc. The bank shall conduct such programs on a regular basis. All education and training programs shall be conducted as per the guideline framed under this policy.

d. Adequacy and effectiveness of Training and awareness programs

The AML Implementing officer shall determine the adequacy and effectiveness of the programs. The bank shall take the Skill Assessment Test (SAT) on trainings provided to the staff to ensure effectiveness of the training programs.

e. Record Retention

The bank shall maintain the record of all education and training programs conducted by the bank. Such record is to kept in a way that it is capable of disclosing name, date, major issues discussed/covered, participants, etc.

3.22 Customer Education:

The cooperation of the customers is the significant factor for the bank to achieve its AML/CFT goals. In order to get utmost cooperation of the customers, the bank shall conduct customer education programs to make them knowledgeable regarding seriousness of money laundering and terrorist financing risks to the bank and ultimately to its customers, why bank asks for various kinds of information from its customers and their vitality for creating a safer bank and so on.

3.23 Cooperation to lawful enforcement agencies

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. Similarly, bank shall ensure that all the instructions and queries received from various enforcement agencies shall be enacted upon the stipulated time. The query handling functions of the bank shall be guided by the procedural guidelines formed under this policy.

3.24 Tipping Off:

The bank or any of its staff shall not disclose to its customer or to any other person that a following report, document, record, notice or information concerning suspected money laundering or terrorist financing or predicate offence has been initiated or is being submitted to FIU and/or any other enforcement authorities and their officers:

- Report of suspicious or threshold transaction
- Order received from FIU or any other enforcement authorities for conducting ongoing monitoring of any customer and make reporting in given time.
- Any document, record or information provided to the FIU and other investigating authorities
- Disclosing name and any other detail of bank staff/s providing report, document or information to concerned authorities

As per provision of ALPA, information shall not be disclosed even in judicial proceedings that discloses or may disclose the introduction of official or staff

ALPA has allowed NRB to fine up to one million rupees fine to the bank if tipping off is done. Similarly, the bank is to take departmental action to its staff as per staff by law.

3.25 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.

3.26 Safe Keeping of customer's transaction record:

The Act requires to maintain the secured record, pertaining to transactions made beyond threshold limit prescribed by Nepal Rastra Bank at a single or in a series of transactions by a

person and any other transaction which appears to be suspicious or transacted with the motive of asset laundering, at least for a period of five years from the date of such transaction. However, the bank shall adopt policy of maintaining full and secured record of activities performed in the process of execution of this policy for a minimum period of seven years even after the termination of relationship with the customer. The detail of documents, information, methods of safe keeping, person wise duties, handling procedure, etc. shall be performed as per the functional guidelines framed under this policy.

3.27 Code of conduct of employees

As a responsible staff of the bank, every staff of the bank shall adhere following code of conduct relating to prevention of money laundering and combating financing terrorism:

- No any staff of the bank (including board members) shall, by any means, be involved in money laundering or terrorist financing directly or indirectly, in part or in whole, unlawfully and willingly
- No any staff of the bank (including board members) shall, by any means, support to money laundering or terrorist financing directly or indirectly, in part or in whole, unlawfully and willingly
- No any staff of the bank (including board members) shall inform/share/talk/disclose/warn, by any means, to any unauthorized persons about the bank's policies and procedures relating ML/FT risk management.
- No any staff of the bank shall inform/share/talk/disclose/warn, by any means, to any unauthorized persons about bank's consideration as suspicious or any investigation initiated by bank or other competent authorities regarding any of its customers or other parties.
- Concerned staff shall provide access to offices or furnish information requested by authorized persons of the bank entrusted with responsibility of legal and regulatory compliances.
- Concerned staffs shall extend full cooperation to the legal and regulating bodies during their investigation in relation to ML/FT activities.

NIC ASIA
एन आई सी एशिया बैंक लि.

- No staff shall provide customer or any third party, at the customers' request, with incomplete or otherwise misleading documents or information in connection with the customer's accounts and transactions

3.28 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.

3.29 Departmental Action:

At each event of violation of the provisions of this policy, the Bank will take departmental action to it staff under staff service by law, 2063

NIC ASIA
एन आई सी एशिया बैंक लि.

Chapter 4

Roles and Responsibilities

4.1 Roles and Responsibilities of Board

The Board of Directors is the apex and supreme authority of the Bank. It is responsible and accountable to frame and implement robust guidelines and frameworks for effective compliance with the laws of land and with the regulations and directives issued by the regulatory authorities. The illustrative but not exhaustive roles and responsibilities of the Board related to this Policy are as follows:

- The Board of Directors shall be responsible for approving the policies ensuring the appropriateness, sufficiency and effectiveness of the policies adopted by the bank based on the overall risk level of the bank on prevention of money laundering and financing of terrorism. Also, the board shall ensure that the Policy Framework is comprehensive for key business and support functions, and establish a method for monitoring compliance of the same.

- The Board shall review the status of implementation of Anti Money Laundering Act, 2064, Anti Money Laundering Rules, 2073, 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.

- 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.

- The Board of Directors of the Bank shall effectively discharge its statutory responsibilities as elaborated hereinabove.

- The Board is authorized to issue appropriate instructions to the senior management regarding Investment Policy that it deems appropriate.
- Any amendments / cancellation or revision in this policy shall be at the sole discretion of the Board.

4.2 Roles and responsibilities of Risk Management Committee (RMC)

Risk Management Committee is the Board level Committee which shall constantly monitor the nature of level of risk being taken by the Bank and how the risk relates to risk appetite and tolerance capacity of the Bank. The illustrative but not exhaustive roles and responsibilities of Risk Management Committee related to this Policy are as follows:

- Review of Reports submitted by Compliance Department on periodic basis.

4.3 Roles and Responsibilities of Chief Executive Officer (CEO):

Chief Executive Officer is the head of the management which shall be primarily responsible for the implementation and ensure effective compliance of the Policies/procedure and guidelines of the Bank/Regulators. The illustrative but not exhaustive roles and responsibilities of Chief Executive Officer of the Bank related to this Policy are as follows:

- Circulate and implementation of the Policy approved by the Board.
- Carry out and manage the Bank's activities in a manner consistent with the business strategy, risk appetite and other guideline provided by the board.
- The CEO shall ensure that the bank has all required procedural guideline in place to effectively achieve the objectives of this policy.
- The CEO shall promote compliance as a culture and consider AML/CFT compliance as a basic ethic of doing business.
- All the procedural guideline containing the controls, monitoring and reporting procedures will be approved by the CEO.
- The CEO shall also ensure that sufficient resources and required access to information, documents and staffs have been arranged to carry out compliance functions efficiently and effectively.
- 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.

- Other discretionary authorities shall be exercised as delegated in the Policy or by the Board from time to time.

4.4 Role and Responsibilities of Chief Operating Officer (COO):

Chief Operating Officer means the Officer or such designated official having other titles of the Bank, who shall be responsible for overall Operations of the Bank. The illustrative but not exhaustive roles and responsibilities of Chief Operating Officer of the Bank related to this Policy are as follows:

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

4.5 Roles and Responsibilities of Business / Department / Unit Heads

- Department/Unit Heads shall be responsible, under the area of their control, for ensuring proper implementation of control, monitoring and reporting activities designed to prevent money laundering and terrorist financing.
- Responsible to reasonably assure that staffs under their control have required knowledge and are not involved in any money laundering and terrorist financing activities.

NIC ASIA
एन आई सी एशिया बैंक लि.

4.6 Roles and Responsibilities of Operation In-charge /Operation Managers

- Operation Managers shall be responsible for ensuring proper implementation of control, and monitoring and reporting procedure across the branch under their control to prevent ML/TF.

4.7 Roles and Responsibilities of Internal Audit Department

Internal Audit Department shall be responsible for check and review effectiveness of this Policy. The illustrative but not exhaustive roles and responsibilities of Internal Audit Department related to this Policy are as follows:

- Internal Audit shall provide independent evaluation of compliance with this policy.
- Internal Auditor shall be responsible for conducting checks and reviews to ensure that the control and monitoring and reporting procedures under this policy.
- Internal audit shall specifically check and verify the application of KYC/AML procedures at the offices/branches and comment on the lapses observed.
- The compliance in this regard shall be placed on the Audit committee and the board at quarterly basis.
- Ensure the process and procedures mentioned in this Policy are duly followed.
- Check the breach of internal and external provision and regulations.
- Conduct the audit as per the provision of NRB.

4.8 Roles and Responsibilities of Legal Department

Legal Department is the department responsible for ensuring compliance to all legal and regulatory requirements as well as all applicable laws of the land related to the Policy in the daily business and operations of the Bank. The illustrative but not exhaustive roles and responsibilities of Legal Department related to this Policy shall be as follows:

- Providing legal opinion as and when required;
- Providing recommendation on statutory and internal requirements on the need basis with regards to the AML / CFT.

4.9 Role and Responsibilities of Human Resource Department

Human Resource Department is responsible for managing overall human resources of the Bank. The illustrative but not exhaustive roles and responsibilities of Human Resource Department related to this Policy shall be as follows:

- HR Department shall ensure that screening against sanction list and due diligence have been made before appointing any person in the permanent and contract positions in the bank.

- HR shall also ensure that due diligence of the employees is updated regularly and record is maintained appropriately.
- Assessment of adequate human resources requirement.
- Training to human resources in the area of AML / CFT on need basis.

4.10 Roles and Responsibilities of Individual Employees

- It shall be the responsibility of every individual employee of the bank to remain vigilant to the possibility of money laundering / terrorist financing risks through use of bank's products and services.
- Any staffs who come to know about the involvement of bank's staff or any of its customers in money laundering or terrorist activities must report to the higher management of the bank following standard procedure framed under this policy and shall be mandatory role of all staffs of the bank.

4.11 Roles and Responsibilities of Branch KYC and AML / CFT Implementing Officer

- Branch KYC and AML/CFT Implementing Officers shall be responsible for executing the duties as required by various guidelines framed under this policy from time to time.
- They shall be primarily responsible for monitoring high value and high risk transactions, detecting suspicious activities and report suspicious transactions/activity to AML Implementing Officer of the Bank.
- The roles and responsibilities of the Branch AML Implementing officers shall be covered in their job description.

Any other responsibility as decided by Board and Risk Management Committee.

Chapter 5

Miscellaneous

5.1 Review / Amendment and Interpretation

This policy shall be reviewed periodically, not exceeding one year from the date of approval / review. Any amendments / insertions shall be recommended to Risk Management Committee for its recommendation to the Board for approval.

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

5.2 Relation of policy with Other Document

This policy must be read in conjunction with the prevailing laws of land pertaining to AML/CFT such as Anti Money Laundering Act, 2064 (with amendments); Anti Money Laundering Rules, 2073; 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 and regulation 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

5.3 Power to Formulate Appropriate Manuals/Guidelines

The CEO is authorized to approve appropriate Manuals/Guidelines required for the effective implementation of the provisions of 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.

5.4 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.

5.5 Repeal & Saving

"Policy for prevention of Money Laundering and Combating the financing of terrorism 2016" approved by the Board of Directors of the Bank vides its 262nd Board Meeting dated: 26th January, 2016 and its amendment (if any) by the Board from time to time shall supersede by this policy.

Except specified otherwise in this document, any amendments/ cancellation or revision in this policy shall be at the sole discretion of the Board.

Any amendment in the laws / rules / regulations / NRB Directives / Circulars affecting provisions under this policy shall have automatic effect amending such provisions under this Policy.

NIC ASIA
एन आई सी एशिया बैंक लि.