Anti -Money Laundering (AML) Policy

NMB BANK LIMITED

October 2019

Version Control :

S. N.	Version	Approving Authority	Approved Date
1	First	NMB Board	April 2008
2	Second	NMB Board	October 2015
3	Third	NMB Board	April 2018
4	Forth	NMB Board	October 2019

Document Classification: Internal

Table of Contents

_Toc33109726

Acronyms

ALPA	Asset (Money) Laundering Prevention Act
AML	Anti-Money Laundering
AMLC	Anti- Money Laundering Committee
AMLPO	Assistant Money Laundering Preventions Officer
BAFIA	Banking and Financial Institution Act
CBO	Chief Business Officer or Chief Business & Strategy Officer
CBS	Core Banking Department
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CFT	Combating the Financing of Terrorism
ECDD	Enhanced Customer Due Diligence
FATF	Financial Action Task Force
FIU	Financial Information Unit
HRD	Human Resource Department
KYC	Know Your Customer
KYE	Know Your Employee
L&D	Learning and Development
ML	Money Laundering
MLPO	Money Laundering Preventions Officer
NRB	Nepal Rastra Bank
PEP	Politically Expose Person
RMA	Relationship Management Application
RMC	Risk Management Committee
STR	Suspicious Transaction Report
SWIFT	Society for World Wide Interbank Financial Telecommunication
TF	Terrorist Financing
TTR	Threshold Transaction Report
UN	United Nations

1. Introduction

1.1 Overview

Money Laundering (ML) is considered as a potent threat to financial system of all countries. The magnitude of its damage extends to a larger dimension in the form of loss of sovereignty and image of a country. This has been now recognized globally and has culminated in concerted efforts to fight against this ultra-criminal activity by way of enactment of stringent laws, regulations and measures aimed at securing financial systems against money laundering.

The financial activities in Nepal is still predominantly ruled by cash based transactions or transactions emanating from non-account holders. There is a significant part of economic activities which are run through informal channels and mechanism and are not in direct control of law enforcement agencies. However, banks and FIs are at some level used by these informal channels to move/route funds inside country or between countries.

There is indeed a need to monitor, control and act against the practices that are directly helping individuals, group and organizations to evade taxes, drugs/human trafficking, finance terrorism and pose threat to national and international economy.

The bank is committed to:

a. Meeting its national and international regulatory obligations in the identification, treatment and management of Money Laundering (ML)/ Terrorist Financing (TF) risk
b. Protecting the bank from reputational risk and breaches of regulatory requirements that may lead to severe actions, fines and penalties
c. Safeguarding the bank, its customers and employees from becoming a victim of, or unintentional accomplice to, ML/TF activities.

1.2 Definition of ML/TF

1.2.1 Money Laundering (ML)

Money Laundering is an activity involving transaction/or series of transactions that is designed to disguise the nature/source of proceeds derived from illegal activities, as

defined in the Anti-Money Laundering Act 2064 2nd amendment on 2070, which may comprise drug trafficking, terrorism, organized crimes, murders, fraud, etc.

It is important for all employees of the Bank to be conversant and familiar with the ML process (described below) as they must be vigilant all the times and should any of the aspects involved in ML process surface in our business they must be able to identify the warnings sign and take appropriate actions.

Placement: The first stage of ML is successfully disposing of the physical cash received through illegal activity. The criminals accomplish this by placing this into a financial institution.

Layering: The second stage concentrates on separation of proceeds from criminal activity through the use of various layers of monetary transactions. These layers are aimed at wiping audit trails, disguise the origin and maintain anonymity for people behind the transaction. E.g. Fraudulent letters of credit transactions, over invoicing for goods transshipped from another country, using high value credit cards to pay for goods/services and accounting for the credit card invoices with balances held in offshore banking secret havens, etc.

Integration: The final link in ML process is sometimes called the integration stage. This occurs when the laundered or cleaned up money is legitimately brought back into financial systems operated by end user and when it is safe and insulated from enquiry by any agency with a legitimate reason for querying the existence of money. E.g. Loan back technique or loan-default technique where the lender bank seeks to recover its assets (loans to money launders) by attaching the securities held by bank which exist in the form of dirty money.

1.2.2 Terrorist Financing

Terrorist financing provides funds for terrorist activity. The main objective of terrorist activity is to cause substantial property or human damage; or seriously interfering with or disrupting essential services, facilities or systems.

There are two main sources of terrorist financing – financial support from countries, organizations or individuals, and revenue-generating activities that may include criminal activities. The second source, revenue generating activities, may involve drug trafficking, human smuggling, theft, robbery and fraud to generate money. Funds raised to finance terrorism usually have to be laundered and thus anti-money laundering processes in banks and other reporting industries are important in the identification and tracking of terrorist financing activities.

Bank shall build measures to monitor, identify and report such funds received or sent using the banks system. Bank shall take caution while doing transaction, account opening or carrying baking activities if in any circumstances the name of any banned organization or individual (involved in terrorist activities) appears as payee/endorsee/applicant and report of such transaction as and when detected.

The Bank shall endeavor to get the list of such organization/individuals to the best possible means or mechanisms.

1.3 Purpose

This NMB AML policy, broadly is based on "Asset (Money) Laundering Prevention Act 2064(2nd amendment on 2070)", Asset (Money) Laundering Prevention Rules 2073 and NRB Unified Directive, Directive number 19. Also this policy incorporates agreed international rules and regulations and best practices, which directs NMB Bank's banking activities to proactively comply with AML prudent practices among its stakeholders.

This policy's purpose is to establish governing standards to insulate the bank from being used as a component of financial system to launder money.

In the light of above, the purposes of the policy are:

a) To enable the bank to conduct clean, commercial business, conforming to standards set by the industry; laws and regulations of the country/governing authorities.
b) To follow, the internationally accepted standards used for Know Your Customer (KYC) compliance, as far as practical.
c) To report and take suitable actions, upon detecting the suspicious activity involving shades of money laundering as directed by Nepal Rastra Bank or any other laws formulated from time to time.
d) To make the employees and customers aware about the seriousness of the impact of ML activities.
e) To set-up administration processes within the Bank to implement the set AML standards.
f) To comply with applicable laws in Nepal with reference to ML and adhere to the standards accepted internationally by the financial world on the subject, as far as practical.
g) To provide the knowledge to identify AML/CFT transactions.
h) To make bank's staff aware of the AML/CFT policies and practices.
i) To avoid the opening of anonymous, UN sanctions list and fictitious accounts.
j) To provide the knowledge to staff to verify the identity of prospective customers before they are allowed to establish account relationship.

1.4 Scope

The four tenets covered in this AML Policy are:

a) Know Your Customer(KYC)
b) Risk Assessment of Accounts
c) Accounts Review
d) Suspicious and large Value Transaction Monitoring and Reporting

This Policy also intends to increase the awareness of ML activities amongst the staff, customers and general public and its ill effects and also effectively counter/guard against ML at all times.

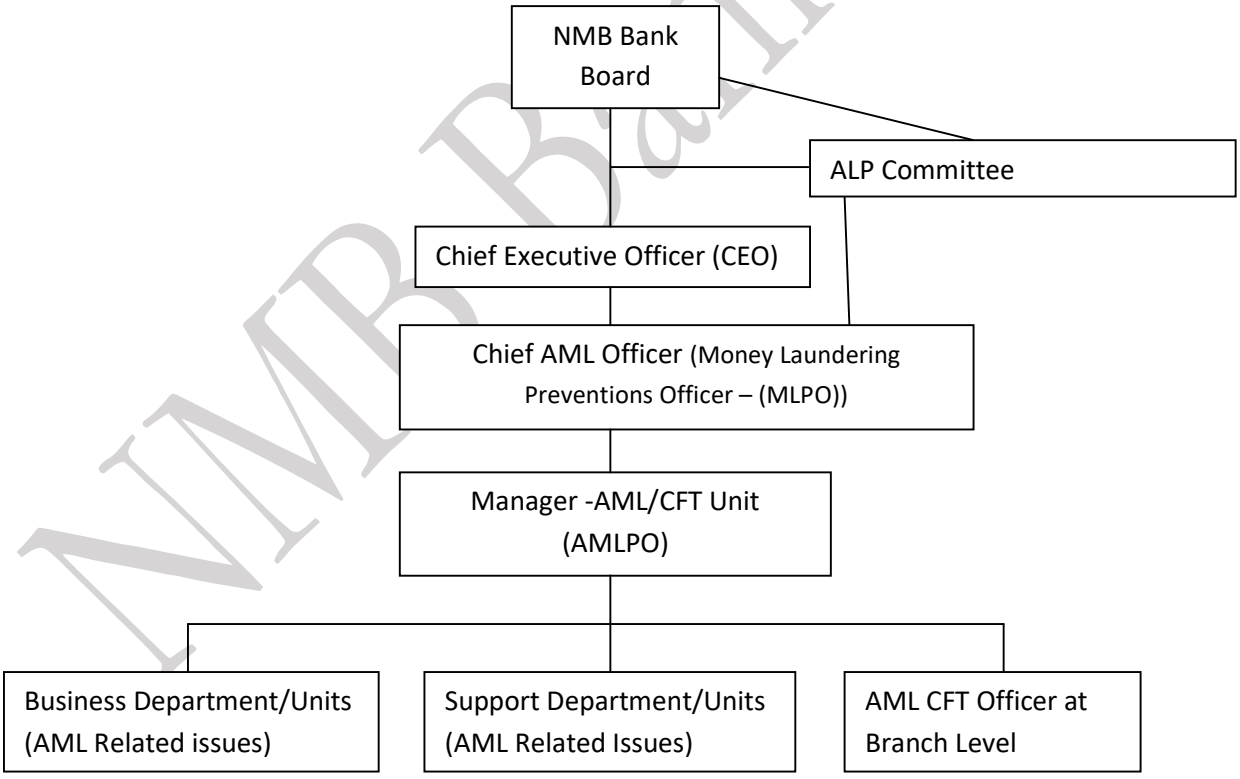
Considering the sensitiveness of the matter on global arena the Bank has developed this Policy in order to be proactive in dealing with issues related with ML within the preview of the local law and guidelines of Nepal Rastra Bank.

Compliance and willing to adopt this policy will be the primary goal while implementing it. All NMB Bank employees and affiliate must comply with this policy.

2. Governance for AML/CFT

Governance structure assigns responsibilities for the effective implementation of bank's AML/CFT policies and monitoring structure and overall accountability.

To align with our business requirements, it incorporates guidance from global standards, NRB circulars and directives and elements consistent with evolving best practices.Compliance governance structure of this policy is at below:



2.1 AML/CFT Governance

2.1.1 Board Responsibilities:

The Board of directors has supreme authority (as directed by ALPA, its rules and NRB Directive) and responsibility to implement robust guideline of the AML/CFT into the Bank. Following are the main responsibilities of the Board of directors:

a. Approving, enforcing internal AML/CFT Policy into the Bank.
b. Establishing and approving the organizational structure, roles and responsibilities in AML/CFT of individual/department/unit.
c. Oversight on the risk management on AML/CFT.
d. The Board of Directors shall review the AML/CFT status of the bank on quarterly basis and provide feedback if any to the management or MLPO.
e. Any amendments/cancellation or revision in the policy shall be the discretion of the board.

2.1.2 Risk Management/AML Committee (Board level) Responsibilities

a. Review and support AML/CFT policy for the purpose of approval from Board of Directors.
b. Review the AML/CFT Status of the bank on quarterly basis and forward to Board for further review.
c. Periodically review and update AML/CFT Policy.
d. Monitoring AML/CFT related activities to implement AML/CFT policy.

2.1.3 Senior Management Responsibilities

2.1.3.1 Chief Executive Officer

Chief Executive Officer is a head of the management of the Bank who ensures that the bank has implemented AML/CFT policy and procedure effectively. Following are the main function of the Chief Executive Officer:

a. Ensuring that policies and procedures for AML/CFT program are in line with changes and developments in products, services and information technology of the bank as well as in line with development in modus for money laundering or terrorist financing.

b. Ensuring that the implementation of AML/CFT program is based on established policies and procedures.
c. Ensuring that all employees, particularly employees of related work units and new employees have participated in ongoing training related to AML/CFT Program.
d. Supervise the AML/CFT unit work in implementing AML/CFT Policy and procedure.
e. Review and approve all AML/CFT Procedures.
f. Based on the recommendation of Money Laundering Preventing Officer (MLPO) for any action to respective staff for not complying AML/CFT Policy and procedure, Chief Executive Officer shall take initiative for further action to such staff.
g. Ensuring that sufficient recourses, suitable work place, required access to information, document and staff have been managed to do compliance function effectively and efficiently.

Other discretionary authorities shall be exercised as delegated in the policy or by the board from time to time.

2.1.3.2 Money Laundering Preventions Officer (MLPO)

Chief AML Officer of the bank shall be the MLPO who shall be the focal point for implementation of the AML Policy, Procedure and regulatory requirements regarding the AML/CFT. Detail information of MLPO like: Name, Address, Qualification, Contact number, Email address shall be sent to Financial Information Unit(FIU) for correspondence. In case of appointment of another staff as Money Laundering Preventions Officer, details of his/her as mentioned above shall be sent to FIU immediately.

AML/CFT Unit:

The Bank shall have a separate AML/CFT Unit under MLPO which shall be implemented of NRB directives, AML ACT/Rules, AML/CFT policy and Procedures. In-charge/Manager of AML/CFT Unit of the bank shall be the Assistant Money Laundering Preventions Officer (AMLPO), who assists to implement entire responsibilities of MLPO

Rights of the MPLO (As per ALPA)

- Direct access to any documents, transactions and document related to accounts.

- Right to demand/acquire any information, details, account statements or documents from any staff of the bank.
- Direct access to any documents, information required for implementation of the ALPA, its rule, NRB Directive and Bank internal policy and procedure.

Responsibilities of MLPO:

- Effective policy, procedure and system shall be developed for the implementation of AML/CFT.
- Suspicious Transaction report which has been sent by Department/Unit/Branch shall be reviewed/analyzed and send to FIU.
- Ensure timely reporting of Threshold Transaction Report (TTR) to FIU.
- MLPO shall consult with other department or get specialist feedback, if needed.
- MLPO shall prepare the report of the AML/CFT status of the bank.
- MLPO shall instruct to bank's management / all departments for complying the AML Policy, Procedure, NRB Directives etc.
- MLPO shall make recommendation to take actions to those staff who have not provided required information, document and account details and/or who doesn't cooperate for the implementation of the AML/CFT to CEO and HR. Details of action taken as mentioned above by bank shall be reported to FIU.
- MLPO shall submit the report of AML/CFT status/implementing of/by the bank to RMC/AMLC and RMC/AMLC shall submit those reports to NMB Board on quarterly basis. NMB Board shall review such report and provide feedback to RMC/AMLC or Management accordingly.
- MLPO shall share the knowledge about the AML/CFT, its impact to the Bank and other details to the shareholders (shareholders who own 2% or more of paid up capital), Board Members, Top level management and staffs. Outsource resource person may also used, if needed.
- MLPO shall facilitate to provide regular training about the AML/CFT to the staff for the improvement of their personal skills and effective implementation in the Bank.
- As prescribe by regulator.

2.1.4 AML/CFT Officer

Designated officer at Unit head of Account Service Operation (ASO) unit and Operation in charge of the respective branches shall act as AML/CFT officer. However, AML/CFT officer of respective branch/unit will be primary responsible to implement of AML/CFT policy and related procedures.

The major responsibilities of AML/CFT Officers will be as follows:

a. To ensure compliance to ALPA, its Rules, NRB Directives along with internal AML Policy and AML/CDD Procedure.
b. To authenticate Know Your Customer (KYC) as required under AML/KYC Procedures.
c. To ensure whether branch/department has obtained required information of Know Your Customer (KYC) at the time of establishing relationship with customer.
d. To maintain record of Know Your Customer information as prescribe under AML/CDD procedure.
e. Send Threshold Transaction Report (TTR) to AML/CFT Unit as prescribe by AML Procedure.
f. To ensure that all staff of the Unit/Branch have carried out in house training on AML/CFT at least once every year
g. Identify the Suspicious Transaction and report to MLPO/AMLPO.
h. To keep customers information confidential at all time.
i. Whilst managing overall AML activities is the responsibility of, AML/CFT officers of respective branches/ Department/ Unit. AML CFT Officer shall liaise with MLPO or AMLPO for any AML/CFT related issues of their respective branches and unit on an ongoing basis.
j. To implement the AML System at Department/Branch/Unit.
k. As directed by the AML Procedure

2.1.5 Head - Operation

Following are the main responsibilities of Head Operation:

a. To ensure proper implementation of ALPA, its rules, AML policy and procedure.
b. To instruct branches/departments to comply the AML/CFT Policy, procedure, NRB Directive, etc.
c. To instruct to respective branches/department for rectifying the discrepancies on AML/CFT related matters.
d. To ensure that all account shall be opened by obtaining required document and information only and input the required information into the Core Banking System (CBS).
e. To make arrangement for digitalization of all customer information as per ALPA/NRB Directive.
f. To instruct to respective unit/branch for account block to implement AML policy/procedure.
g. As directed by the AML/CDD Procedure.

2.1.6 Chief Business Officer (CBO) and Head of the Department

Following are the main responsibilities of Chief Business Officer (CBO) and Head of the Department:

a. Chief Business Officer (CBO) and Head of the Department shall be the responsible of their own respective department/unit /branch for ensuring proper implementation, control, monitoring and reporting activities designed to prevent money laundering and terrorist financing as per ALPA/ its rules/AML policy/ procedure.
b. Responsible to reasonably assure that staffs under their control have required knowledge and are not involved in any money laundering and terrorist financing activities.
c. As directed by the AML/CDD Procedure.

2.1.7 Branch Manager

Following are the main responsibilities of Branch Manager:

a. To ensure proper implementation, control, monitoring and reporting procedure across the branch under their control to prevent Money Laundering and terrorist financing.
b. To ensure that all customer related documents of Account Opening/KYC form including transaction shall be kept in prescribe way and provide to Compliance Department or AML/CFT Unit or authorized authority as per BAFIA immediately or as and when required.
c. To ensure all staff of the branch have gone through in-house training on AML/CFT at least once every year. If not, Branch Manager shall escalate that information to Learning & Development Department for providing training to those staff.
d. Responsible to reasonably assure that staffs under their control have required knowledge and are not involved in any money laundering and terrorist financing activities.

e. Branch Manager shall be primarily responsible for monitoring high value and high risk transactions, detect suspicious activities and report suspicious transactions/activity to MLPO/AMLPO.
f. As directed by the AML/CDD Procedure.

2.1.8 Information Technology Department (IT)

IT Department is responsible to provide necessary data and support to AML& CFT Unit & Integrate customer /transaction details into AML System and back up of AML system to maintain on daily basis.

2.1.9 Internal Audit Department

Internal audit is an independent body which shall be tested whether bank has effectively followed the ALPA/its rules, NRB Directive and AML/CDD policy and Procedureof the bank. Following are the main role and responsibility of Internal Audit Department:

a. Internal Audit Department shall independently review the compliance of AML Policy and procedure.
b. Internal auditor shall be responsible for conducting checks and reviews to ensure that the control and monitoring and reporting procedures under this policy.
c. Internal audit shall independently checks and verify the AML Policy and procedure of the bank, ALPA/its rulesand NRB Directive at department/ branch/unit and report it accordingly.
d. Compliance on AML/CFT and updated status of department/branch/unit, shall be provided to AML/CFT unit on quarterly basis.

2.1.10 Human Resource Department (HRD)

Following are the main role and responsibility of Human Resource Department:

a. To screen the staff on AML Prospective (criminal activities, sanction list etc.) before recruitment of staff. It is also applicable for outsource staffs.
b. HR shall ensure that the due diligence of all employees is updated regularly and record those details into CBS.

c. Transaction of all staff shall be monitored by HR department to identify ML activities.
d. HR shall arrange a training program related to AML/CFT to staffs on need basis.
e. Departmental punishment/action as recommended by MLPO/CEO, shall be taken to those staff that does not comply the NRB directives and AML policy/procedures.

2.1.11 Learning and Development Department (L&D)

Following are the main role and responsibility of Learning and Development Department:

a. To arrange trainings related to AML/CFT to all staff at least once a year.
b. To facilitate to provide national and international training on AML/CFT to MLPO, staffs of AML/CFT Unit and any staff who directly involve in AML/CFT activities.

2.1.12 Individual employee

Following are the main role and responsibility of individual employee:

a. Individual employee shall be more vigilant to possibility of money laundering/terrorist financing risks through the use of bank's products and services.
b. Any staff who come to know about the involvement of bank's staff or any of its customers in money laundering or terrorist activities must be reported to the MLPO/AMLPO of the bank.

3. Know Your Customer/ Employee

3.1 Know your customer (KYC):

KYC is the process of a business verifying the identity of its clients. The term is used to refer to the bank regulation which governs these activities. Banks are increasingly demanding that customers provide detailed anti-corruption due diligence information, to verify their probity and integrity. Know your customer policies are becoming much more important globally to prevent identity theft, financial fraud, money laundering and terrorist financing. NMB shall not engage in business relationship for which customer identification and KYC is not performed.

3.1.1 Customer Acceptance Policy (CAP)

Bank's customer Acceptance Policy (CAP) lays down the criteria for acceptance of Customers.

a. Account shall be opened only in the name of natural and legal person/organization, the name being the same as in the primary identify document as describe in AML Act, Rule, NRB Directive 19, Bank's AML CDD Procedure, of the person/entity. Bank shall only open the account on the basis of required Document and Information as describe in AML Act, Rule, NRB Directive 19, Bank's AML CDD Procedure.

b. Account shall be opened after identification of customer and verification of required information/document. Necessary checks are done before opening a new account so as to ensure that the identity of the customer does not match with any person with money launder or with banned entities such as individual terrorists or terrorist organizations etc.

c. P. O. Box addresses are not acceptable as a recorded residential address. (P. O. Boxes are acceptable as mailing address).

d. Accounts must not be opened or retained (or one-off transactions undertaken) where it is known or suspected that a customer or prospective customer is involved in money laundering or terrorist financing. In such circumstances the account opening process should cease and, where appropriate, a Suspicious Activity Report (SAR) should be reported to MLPO or AMLPO.

e. The bank shall not open accounts for shell banks or hold alternate name anonymous (altering form the primary identity document) or fictitious (Benami) name or Blank name or numbered/alphanumerical characters accounts. Any such existing accounts must be exited.

f. Accounts shall not be opened, or one-off transactions undertaken, for sanctions listed individuals or entities.

g. In case, power of attorney holders, third party mandates or guarantors in a relationship, such persons should be identified in the same manner as the primary

customer. The documents for such arrangement should be verified and the reason for the arrangement understood and recorded.

3.2 Purpose of KYC

a. To establish procedures to verify the identification of individuals or corporate or other institutional accounts.
b. To detect suspicious transaction.
c. To establish process and procedures to monitor high value and suspicious transactions.
d. Establish systems for conduction due diligence and reporting of such activities.

3.3 Mechanisms Deployed for KYC

The bank shall use various mechanisms for Customer Due Diligence/ Know Your Customer. These activities shall be carried out at the time of account opening for all the types of accounts opened by NMB bank. Bank shall deploy all or the combination of any of the below mechanisms for KYC/CDD.

a. Customer identification and Profiling
b. Risk Assessment
c. Documentary Evidence
d. Verification of Documents as per original
e. Identification of Beneficial Owner
f. Politically Exposed Person (PEP) verification
g. Restriction on Account Opening

3.3.1 Time line for obtaining KYC

KYC of the customer can be obtained after establishing a business relationship or doing any transactions in the following cases after approval of Respective Chief Business Officer:

a. If bank can ensure that the customer can be identified and KYC can be obtained anytime within short notice.
b. If it is not possible to obtain KYC or business gets interrupted and where it is not necessary for such interruption.

c. If the risk related to money laundering and terrorist financing does not exist with the customer or customer business.

Notwithstanding anything contained in the above, KYC has to be obtained in prior to account opening/transaction in the following conditions:

a. If the customer is a high risk or PEP or a family member or relative to a PEP.
b. If the customer or transaction seems suspicious and high value transaction.

3.4 Know your customer for High Risk account

Banks shall ensure whether the customers, beneficiary owner and potential customer are high risk customer or not. Risk management procedure for High risk customer shall be described in the AML CDD Procedure under Risk assessment section.

In case of local/foreign customers who are high authority persons or PEPs or customers of foreign organization with high risk on the basis of their business or in case of citizen who are high risk customers, the following conditions shall be followed:

a) Approval of respective Chief Business Officer (CBO) must obtain before establishing business relation. CBO can delegate his/her high risk account approving authority to managerial level staff as per Human Resource Bylaws during the period of his/her absent (leave, business trip etc.)
b) If the existing customer falls under high risk customer, approval as per above clause (a) must be obtained immediately.
c) Bank shall identify the source of fund of high risk customer or beneficial owner.
d) Ongoing monitoring of the business relation with the customers and their transactions.
e) Conduct enhanced customer due diligence (ECDD) of such high risk customer.

3.4.1 Enhanced Customer Due Diligence (ECDD)

Bank shall obtain the ECDD in following conditions:

a. High risk customer
b. Customers of high risk country or partially implement FATF standards.
c. PEPs, his/her family members and close associate person or falls under PEP.
d. Customer who makes huge value of transaction, complicated and unnatural in nature whose financial or legal objective is not clear.

e. A customer whose business relation or transaction with individual, company or any legal entity which has not fully or partially followed the FATF standard or high risk country.
f. Customer who use the new technology which is the potential risk for ML/TF.
g. Customer who is suspected for ML/TF.
h. As prescribe by regulator.

3.5 Simplified Know Your Customer

In case of customers and account transactions with low risk grade with respect to money laundering and terrorist financing perspective, simplified KYC can be done under following conditions:

a) Simplified KYC shall not be allowed in case of high and medium risk customers and transaction above NPR 100,000.00 (one hundred thousand) within a year or in case of any kind of suspicions exists regarding money laundering and terrorist activities.
b) Other provisions regarding simplified KYC shall be done as per the regulatory requirement.

3.6 Provisions regarding KYC of existing customers

In case of existing customers maintaining account and/or doing transactions before implementation of this policy, customer shall be identified, documents shall be reviewed and risk grading shall be done on the basis of customer and/or beneficial owner, business relations, transactions, manufacturing or service details, country or geographical region or its distribution methods as per this policy. The mentioned review shall be done within the time frame given by NRB.

3.7 Beneficial Owner

Beneficial owner means the ultimate natural person who owns or controls money or property or customer or (on whose interest the transaction is carried out). It also means the ultimate natural person who controls or exercises such powers to a legal person or arrangement. Identity of such beneficial owners must be established in line with the AML CDD Procedure on following conditions:

a. If the transaction is done on behalf of actual customer.
b. If bank identifies that the transaction is done by someone else other than the actual customer.

Bank shall open an account only if the beneficiary owner can be identified. If the bank could not identify the beneficiary owner or customer is unable to provide the information of beneficiary owner, relationship with any person or entity shall not be established.

3.8 Know your Employee (KYE)

NMB bank shall have processes in place that provide reasonable assurance of the identity, honesty and integrity of prospective and existing employees. These processes are being enhanced within timeframes as per the NRB Directive. Human Resource department shall incorporate the provision of KYE in their recruitment process and the KYE of the employees shall be reviewed annually or as provision set by the regulator.

4. Prevention of Money Laundering (ML)/Terrorist Financing (TF)

This policy is representing the prevention of ML/TF risk by the bank.

The bank is committed to fully comply with the applicable rule and regulation of AML/CFT of the country. The bank also adopts not only the AML/CFT rules of existing country but it shall be adopted international best practice as applicable. Senior management has fully committed to establish appropriate Policy and procedure as per requirement of the ALPA, its Rules and NRB Directive. Senior management shall also facilitate to implement these policies and procedure into the bank and make arrangement to monitor and control risk arising from money laundering/terrorist financing activities in its daily operation and business transactions. 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 Money Laundering/Terrorist Financing risk which cannot be mitigated effectively.

4.1 New Technologies

a. Banks shall assess the money laundering and terrorist financing risk arising from new technologies and business practices on banking, non face to face banking and other new technologies regarding development.

b. Risk assessment in the above case must be done before implementing such new technologies, business practices or distribution system.

c. Bank shall prepare proper method for the management of risk arising from the above process before implementing such new technologies into the Bank.

d. Banks shall develop a procedure for the mitigation of risk arising due to non - face to face banking with customer.

4.2 Anti-bribery and anti-corruption

NMB Bank is committed to ethical business. The policy is never to offer, pay request, solicit or receive bribes, or to facilitate, assist in or abet any offer or payment of bribes and to refuse any request to pay them. Bribery may expose the group to criminal or regulatory investigations that may result in prosecution, fine and costs to our business. Bribery may also expose the group to legal action from competitors or third parties. Individuals engaged in corrupt behavior are likely to face criminal prosecution personally. Receiving bribes or bribing can never be accepted regardless of its purpose.

4.2.1 Corruption

Corruption is demanding, offering, giving or accepting any kinds of bribe or illegal benefits that would cause deviations in the lawful performance of duties or necessary actions by a person, who directly or indirectly acquires the illegal benefit or bribe.

4.2.2 Bribery

Bribery is a person's gaining benefit within the framework of an agreement entered into with a third party so that such person acts in breach of the requirements of his/her duty by performing or not performing a work, speeding up or slowing down thereof, etc.

Bribery and corruption may occur in various different ways and fields, such as:

- Gifts
- Political Donations
- Hospitality
- Outsourcing Companies and Business Partners
- Facilitation Payments

4.2.3 Bribe

A "bribe" is defined broadly and may include any financial or other advantage, including the provision of a service or anything of value. A bribe may include financial payments, whether in cash or cash equivalent (such as gift certificates), or non-cash benefits in kind such as gifts, services, loans, travel, meals, lodging valuable security, property or any interest in property of any description, protection from penalties, the release from any obligation and entertainment. A bribe may also include the provision of anything of value for inadequate consideration.

The Source of fund from bribery and corruption is also known as Money Laundering activities

5. Risk Assessment

a) Bank shall analyze the customer profile on the basis of country of origin, geographical region, nature of business, occupation, type of customer, service or product, transaction and delivery channels for the risk assessment for the Money laundering and Terrorist financing.
b) Bank shall also follow the basis of national risk assessment or risk assessment by regulatory authority after receiving national risk assessment report.
c) Bank shall identify the risk grade based on the above mentioned section (a) criteria.
d) Bank shall record such assessment and report to regulatory authority as per NRB directives and also report such assessment when it is required by authorize body.
e) Bank shall segregate the customer in different category (high, Medium, low, etc.) as per their risk level and assessment shall be done as same.

6. Suspicious and Large Value Transaction

This section of the document is intended to highlight about the suspicious transaction and large value transaction. The Bank will refuse any transaction where based on explanation offered by the customer or other information, reasonable grounds exist to suspect that the funds may not be from a legitimate source or are to be used for an illegal activity such as terrorism, human trafficking etc. The bank shall use reasonable judgment in determining the suspicious transactions.

The understanding of customers' identity vis-à-vis his stated norms of dealings, services, etc would also have a bearing on transactions before they are viewed as suspicious transactions hence cautious approach in the process is very essential. Under no circumstances, bank will alert a customer about his transactions being considered suspicious or that reporting is underway. The Bank will make prompt report of suspicious transactions, or proposed transactions to Financial Information Unit (FIU) through MLPO.

Bank shall report a suspicious transaction within given deadline as per NRB directive of identifying any suspicious customer, transaction or property in the following cases:

1. In case of any suspicion of any charges relating to money laundering and terrorist financing or suspected for any other charges or any ground for consider suspicion.
2. If a person or organization is suspicious of involving in any Terrorist Financing or a part of any terrorist group or has done any financing related to terrorist activities.

Suspicious transaction reporting shall be done even in case of any attempts of doing transactions related to money laundering and terrorist activities.

Additional provisions for suspicious transactions, format of suspicious transaction reporting, reporting methods and procedures shall be prescribed in the AML/CDD Procedure.

7. Wire Transfer

Wire transfer is a method of electronic funds transfer from one person or entity to another. A wire transfer can be made from one bank account to another bank account within the national boundaries of a country or from one country to another. In wire transfers do not involve actual movement of currency, they are considered as a secure method for transferring fund from one location to another. Detail procedures related to wire transfer shall be prescribed in the AML/CDD Procedure.

8. Correspondent and Shell banks

8.1 Correspondent banks

NMB shall implemented risk based due diligence procedures that include, but are not limited to, the following – understanding the nature of the correspondent's business, its license to operate, the quality of its management, ownership and effective control, its AML Policies, external oversight and prudential supervision including it's AML/CFT regime. The Bank

shall conduct required due diligence while establishing SWIFT Relationship Management Application (RMA) with any correspondent Banks.

Additionally, ongoing due diligence of correspondent accounts shall be performed on a regular basis or when circumstances change. Bank policies also ensure that we do not offer 'payable through accounts'. All correspondent banking relationships are approved by senior management of the bank.

8.2 Shell Bank

A shell bank is a financial institution that does not have a physical presence in any country. NMB Bank shall not conduct business with shell bank.

9. Account and Transaction Monitoring

Banks shall carry out ongoing due diligence of customers, beneficial owners or transactions by performing the following actions:

a. Checking whether or not the transaction has been done as per the description provided to the bank regarding the business and its risk until the relationship lasts and obtain information about the source of income if necessary.
b. In order to ensure that the documents and information about the Political Expose Persons (PEPs) or high risk individuals are sufficient by updating the records through review.
c. Regular inspection of relationship with customer and their transactions related to wire transfer and cross border through correspondent banking.
d. Other functions prescribed by the regulatory authority.

The process (automated or manual) of monitoring transactions after the execution to identify unusual transactions, including monitoring single transactions as well as transaction flows, for subsequent review and, where appropriate, report to the authorities. The purpose of transaction monitoring is to provide ongoing identification of suspicious activity from customer transaction data.

Bank shall give special care on providing the following transactions:

a. All transactions which are huge, complicated and unnatural in nature whose financial or legal objective are not clear.

b. Business relation or transaction with individual, company or any legal entity which has not fully or partially followed the FATF standard or high risk country.
c. Any other transaction mentioned by the regulatory authority.

Investigations shall be done as much as possible in case of above transactions identified and record of the same shall be kept.

10. Reporting Related to AML/CFT

When detecting suspicious transaction or having the reasonable grounds to suspect the account transaction has derived from the illegal activity or in relation with money laundering, AML/CFT Unit must report to FIU under the confidential mode. Process for raising the STR and report to FIU shall be described in the AML/CDD Procedure of the Bank.

Bank shall also generate TTR (Threshold Transaction Reports) and other reports related to AML/CFT and report it to FIU/regulator as requested by them or provision in the Directive/circular.

11. Provisions regarding restriction in transactions:

Business relationship shall not be maintained or transactions shall not be done in the case of the following customers:

a) Customer not providing necessary information and documents regarding identification of customer as per AML/CDD Procedure.
b) Customer who could not be identified from the information and details obtained from the customer.

Business relationship must be stopped in case the existing customers falls under the clause mentioned above.

12. Retention of Records

In terms of the operating procedures of the Bank, records such as Account Opening/KYC Forms, vouchers, ledgers, registers, etc., pertaining to Banking Transactions for specified periods are required to be maintained.

a) To assist the authorities on investigation of cases of suspicious money laundering, it is essential that evidence of customer identification, address, transactions details are retained by the bank as mandated by the regulators. Such records must be archived in a

secure area under the custody of a dedicated custodian. Access to such records must be made available only with due approval from Head- Operation or authorized staff by him/her.

1. Records of every transaction undertaken for/by a customer must be retained for 7 years.
2. Account Opening/KYC details information of customer, beneficiary owner/Closing forms/ATM/Mobile/Internet banking requests of the customers must be retained for 7 years from the date of closure.
3. Documentary evidence of any action taken in response to internal and external reports of suspicious transactions, STR related documents, Wire Transfer related transaction must be retained for 7 years from the date of closure.
4. Where it is known that an investigation is ongoing, the relevant records must be retained until the authorities inform the Bank otherwise.

b) Notwithstanding anything contained in the mentioned clauses above, documents and records shall be maintained for at least 7 years and can be maintained for additional period as prescribed by other policies.
c) The records must be retained in a way that the transaction is clearly visible & all records should be easily available as evidence when required.
d) Other provisions regarding retaining the records shall be as prescribed in the act, regulation, NRB Directives.

13. Confidentiality of Customer Information (Tipping Off)

Bank's staff shall not disclose the customer information such as report, document, record, statement and information which are prepared as per the AML/CFT Act, Rule and NRB Directive 19 to other customer or any other unauthorized persons. The concerned staffs shall take utmost precautions that they do not leak such confidential information. Tipping Off is a punishable offence.

14. Policy Compliance

14.1 Employee Training Program

Training shall be provided to business units that offer products and services that are subject to the legislative requirements. Staff involved in customer facing areas, remittance, SWIFT etc, of the bank shall receive periodic training and reminders on the detection and reporting process for suspicious activities. Communication of changes to AML/CFT legislation or any emerging risks are communicated to the relevant staff.

In addition to the above, Human Resource Department/Learning and Development Department shall make sure that the training on AML/CDD will also be provided to all the staff using internal or external.

14.2 Branches and subsidiary companies:

a. Branches in Nepal or any other country and all the subsidiary companies holding more than 50% share holding shall be liable to follow the AML policies and procedures formulated as per AML Acts and Rules & their regulatory instruction.
b. Following subject matters must be followed for the implementing AML CFT.
    1. Conveying information regarding identification of customer and risk management related to money laundering and terrorist financing.
    2. Conveying information regarding programs related to customer, transactions, account, audit, compliance and AML & CFT.
    3. Utilization and Confidentiality of the information conveyed as per above mentioned clauses.
c. If the regulation of any country in which our branches and subsidiaries as per clause mentioned in (a) and (b) above belongs raises any obstructions, it shall be immediately reported to the regulatory body and provisions regarding implementation of AML & CFT policy shall be implemented.
d. If the provisions mentioned in clause (c) above are not sufficient to prevent money laundering and terrorist financing, then the branches and subsidiaries located in the country must be closed.

14.3 Amendment to the policy

NRB and FIU may issue the AML related circular/directives from time to time and the AML Act and Rules of the country shall form integral parts of this policy. If any section/sub-section/clause of this policy contradicts with the country's laws, FIU/NRB's directives, circular; shall be valid to the extent of contradiction.

This policy is subject to review annually or as required for updates in the terms or any clause of the policy. There shall be a separate AML/KYC procedure formulated by the Bank and implemented after approval of Chief Executive Officer.

14.4 Compliance Measurement

MLPO or the designated officer will verify compliance to this policy through various methods, using various tool, reports, internal and external audits, and feedback to the policy owner. Banks auditors shall conduct programs of audits and compliance testing of this policy and operational procedures applicable to AML. The frequency and scope of the audits and compliance tests are determined through a risk-based approach, where higher risks to NMB are audited and tested more frequently.

Similarly, AML/CFT Unit or Compliance department shall conduct assurance review in some branches/departments on sample basis for the compliance test of this policy.

14.5 Exceptions

Any exception to the policy must be acknowledged by MLPO and approved by the bank management.

14.6 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, as per the provisions in the prevailing NMB Bank Employee Bylaw.

14.7 Repeal and Saving

4.7.1 Anti Money Laundering Policy version 3, is here by repealed.

4.7.2 Activities carried out related AML monitoring, implementation, reporting etc, under Anti Money Laundering Policy Version 3 shall be considered as done under this policy.