NMB BANK LIMITED
एनएमबि बैंक लिमिटेड
("A" class commercial bank licensed by Nepal Rastra Bank.)

Bank of the Year, ASIA 2021
Bank of the Year, Nepal
2017, 2018, 2020 & 2021

AML POLICY

(Version 8)

NMB Bank Limited

July 2025

Revision History & Version Control

Sn	Version	Approving Authority	Date of Approval
1	1st	152nd Board Meeting	May 8, 2008
2	2nd	298th Board Meeting	October 9, 2015
3	3rd	356th Board Meeting	June 1, 2018
4	4th	392nd Board Meeting	October 17, 2019
5	5th	422nd Board Meeting	July 6, 2021
6	6th	444th Board Meeting	23 December 2022
7	7th	467th Board Meeting	May 10, 2024
8	8th	497th Board Meeting	October 10, 2025

Document Classification: Internal

Table of Contents

Acronyms

ALPA	Asset (Money) Laundering Prevention Act
ALPC	Assets Laundering Prevention Committee
AML	Anti-Money Laundering
AMLPO	Assistant Money Laundering Preventions Officer
BAFIA	Banking and Financial Institution Act
CBS	Core Banking System
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CFT	Combating the Financing of Terrorism
DCEO	Deputy Chief Executive Officer
ECDD	Enhanced Customer Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
HRD	Human Resource Department
KYC	Know Your Customer
KYE	Know Your Employee
ML	Money Laundering
MLPO	Money Laundering Preventions Officer
NRB	Nepal Rastra Bank
PEP	Politically Exposed Person
PF	Proliferation Financing
RMA	Relationship Management Application
RMC	Risk Management Committee
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
SWIFT	Society for World Wide Interbank Financial Telecommunication
TF	Terrorist Financing
TTR	Threshold Transaction Report
UN	United Nations
WMD	Weapons of Mass Destruction

1. Introduction

1.1 Overview

Money Laundering (ML) is considered as a critical 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 concluded in rigorous 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 Government of Nepal has enacted the Money (Asset) Laundering Preventions Act 2064 (ALPA), to prevent money laundering and provide for confiscation of property derived from, or involved in money laundering. Further, the government has made amendments vide Money (Asset) Laundering Prevention Act 2068, 2070, 2072, 2075 and recently on 2080. The government of Nepal has also issued Money Laundering Preventions Regulation on 2081.

The Nepal Rastra Bank (NRB) hereinafter referred as “Regulator” issues directions on KYC standards (NRB Directive, directive number 19) for banks and financial institutions, last updated on 2081-09-29. Financial Intelligence Unit (FIU) - Nepal is a national agency responsible for receiving, processing, analyzing and disseminating financial information and intelligence on suspected money laundering and terrorist financing activities to the relevant law enforcement/investigative agencies and foreign FIUs.

The financial activities in Nepal is still predominantly ruled by cash based transactions or transactions coming out 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.

However, due to rapid digitization move after covid period, the trend has shifted from cash based to electronic based (web, mobile, card, digital wallets etc), a significant leap on used of digital platform for transactions purpose.

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 facilitate proliferation financing, which involves providing financial

support for the development and spread of weapons of mass destruction (WMD), thereby posing a significant 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 and Proliferation Financing (PF) 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 ML/TF activities or from being unintentional accomplice (collaborator) to such crime or wrongdoing.

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, recent amendment in 2080, which may comprise drug trafficking, terrorism, organized crimes, 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. During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos and other legitimate businesses, both domestic and international.

Examples of placement transactions include the following:

- Blending of funds: Commingling of illegitimate funds with legitimate funds, such as placing the cash from illegal narcotics sales into cash-intensive, locally owned restaurant
- Foreign exchange: Purchasing of foreign exchange with illegal funds
- Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade reporting requirements

- Currency smuggling: Cross-border physical movement of cash or monetary instruments
- Loans: Repayment of legitimate loans using laundered cash

Layering:

The second stage concentrates on separation of proceeds from criminal activity through the use of various layers of monetary transactions, intended to conceal the origin of the proceeds. These layers are aimed at wiping audit trails, disguise the origin and maintain anonymity for people behind the transaction.

Examples of layering transactions include:

- electronically moving funds from one country to another and dividing them into advanced financial options and/or markets;
- moving funds from one financial institution to another or within accounts at the same institution;
- converting the cash placed into monetary instruments;
- reselling high-value goods and prepaid access/stored value products;
- investing in real estate and other legitimate businesses;
- placing money in stocks, bonds or life insurance products; and
- using shell companies to obscure the ultimate beneficial owner and assets.

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 for 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.

Examples of integration transactions include:

- purchasing luxury assets, such as property, artwork, jewelry or high-end automobiles; and
- getting into financial arrangements or other ventures where investments can be made in business enterprises.

1.2.2 Terrorist Financing

Terrorist financing provides funds for terrorist activity. The main objective of terrorist activity is to cause substantial damage to property/human; 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 banking 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.

1.2.3 Proliferation Financing

Proliferation financing (PF) refers to the financial support provided for acquiring, developing, or exporting WMDs, including nuclear, biological, and chemical weapons. It remains a global concern, with international bodies such as the United Nations (UN) and FATF enforcing strict measures to curb these activities. Nepal, though distant from global proliferation concerns, must continue strengthening safeguards to prevent any misuse of its financial system for proliferation financing purposes.
Mitigating proliferation risk involves international cooperation, robust regulatory frameworks, intelligence sharing, and effective enforcement measures to prevent the spread of WMD and ensure global security.
Bank shall conduct CDD measures to assess the background of clients and the nature of client's business and its potential involvement in sectors that may be associated with WMD development. Bank shall also establish systems to monitor transactions for unusual patterns or activities that may indicate proliferation financing, such as large cash transactions, transfers to high-risk jurisdictions, or transactions involving dual-use goods.

The bank shall regularly screen clients and transactions against national and international sanctions lists related to proliferation, such as those maintained by the United Nations (UN), United Kingdom (UK), the European Union, and the U.S. Office of Foreign Assets Control (OFAC).

1.3 Purpose

This NMB AML policy, broadly based on "Asset (Money) Laundering Prevention Act 2064 (recent amendment in 2080)", Asset (Money) Laundering Prevention Rules 2081 and NRB Unified Directive, Directive number 19. The policy also 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 protect 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 serious 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 listed 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 Monitoring & 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 thereby to effectively counter/guard against ML at all times.

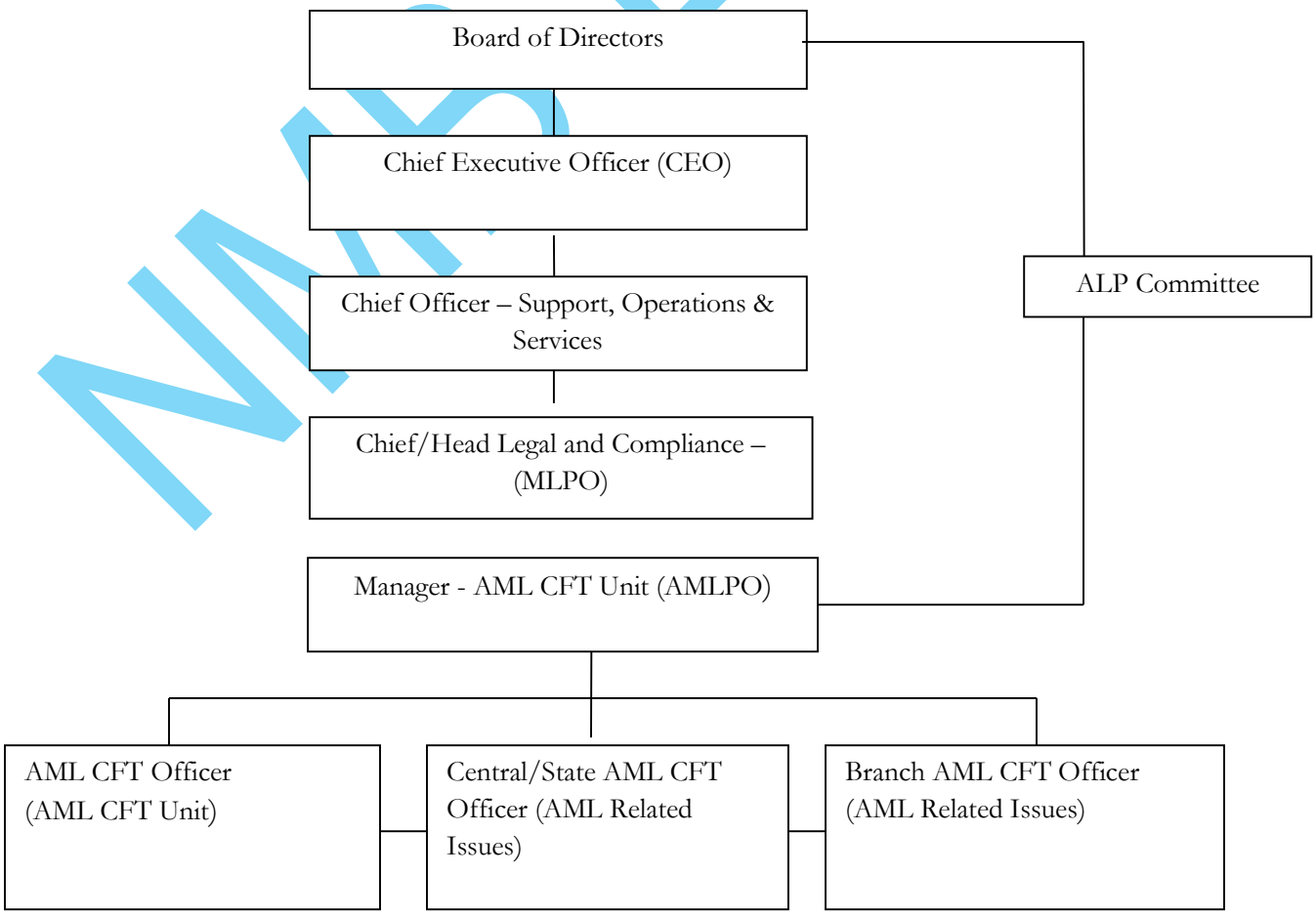
Considering the sensitiveness of the matter on global arena, the Bank has developed this Policy in order to be proactive in dealing with issues related to ML within the purview of local law, its' guidelines and NRB's directive.

Complying 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.
c. Oversight of 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 Asset Laundering Prevention Committee (Board Level) Responsibilities

The ALPC shall assist the Board of Directors in fulfilling its oversight responsibility over the bank's compliance management to make sure that the bank complies with the provision of the Assets Laundering Prevention Act (ALPA), 2064, its rules 2081, NRB directives and Bank's AML Policy and Procedure to the end that the bank shall not be used as a vehicle to legitimize the proceeds of unlawful activity or to facilitate or finance terrorism.

NRB directive no 6 has separately defined the responsibility of ALP committee as below:

1. The committee shall review the report related to the implementation of Money (Asset) Laundering Prevention Act 2064, Money Laundering Prevention rule 2081, NRB Directive (directive no. - 19) at Bank and submit those reports to NMB Board.
2. The Committee shall discuss on the appropriateness and adequacy of the internal policies and procedures in place by the Bank as per the rationale of Money (Asset) Laundering Prevention Act 2064, Money (Assets) Laundering Prevention Rules 2081, NRB Unified Directive (directive no. - 19) and Financial Action Task Force (FATF) recommendations; make needful policy and procedural arrangements and ensure implementation of the same.
3. The Committee shall discuss and provide opinion to NMB board on the requirement and adequacy of the procedural arrangements in place and the information technology system adopted/to be adopted by the Bank for implementation of such arrangements in order to ensure effective

Identification and prevention of Money Laundering and Financing of Terrorism.

4. The committee shall analyze the Customer Identification Procedures of the Bank so as to ensure that the risk-based customer identification and customer acceptance procedures are formulated and under implementation based on the risk categorization of the customer including the PEPs and Ultimate Beneficial Owners and implement effectively.
5. The Committee shall submit the report related to the status of implementation of Money (Asset) Laundering Prevention Act 2064, Money Laundering Prevention Rule 2081, NRB Directive/Circular related to AML/CFT and Bank's AML Policy and Procedure, to the NMB Board on quarterly basis.
6. The committee shall receive following details/reports from the management and suggest as necessary to the NMB Board:
   a. Anti-money Laundering (AML) and Countering the Financing of Terrorism (CFT) Risk Management Report.
   b. KYC Update Status of the Customer, Details of Customer Due Diligence (CDD), Details of PEPs, Details of Enhanced Due Diligence (ECDD) and policy, procedures and institutional measures to be adopted by the Bank for ensuring promptness and effectiveness of KYC update and due diligence measures by use of Information Technology.
   c. Detailed Review report on observations/comments/remarks concerning issues of money laundering and financing of terrorism as mentioned in the Internal Audit Report, External Audit Report and NRB Inspection Report and further courses of action taken/to be taken with regards to such comments.
7. The committee shall direct/assist management on the inherent risks of money laundering and terrorism financing associated with Launching/initiating new services/facilities, purchase of IT System, initiating wire transfers (including mobile banking, internet banking and QR Code), transfer of funds through mobile banking (mobile wallet), online/offline transactions, etc. and further suggest/recommend necessary improvements on the policies and procedural arrangements adopted by the Bank for effective management of such risks.
8. The Committee shall analyze the potential impacts on the Bank arising from incidents related to Money Laundering and Financing of Terrorism, both at the national and international levels and recommend necessary suggestions to the NMB.

9. The committee shall make necessary arrangements to manage a program for providing appropriate knowledge of AML and CFT to the AML Implementing Officer, Shareholders holding 2% or more shares of the Bank, Board of Directors, Top Level Managements and staffs actively/regularly involved in jobs concerning to AML and CFT.
10. The Committee shall review the Policy and Procedure on regular basis on AML and CFT and ensure for effectively implement such provision at Bank and submit such report to NMB Board.
11. The committee shall ensure the effectiveness of AML and CFT mechanisms in place, effective management of ML/FT risk, adequate monitoring of unnatural activities and submission of requisite reports to respective body/authority, and also make necessary arrangement to discuss the same in board meetings.
12. The committee shall discuss on the issue that all the reports and details concerning AML and CFT to be submitted to various authorities are being submitted on a regular basis through the medium as specified by the FIU and NRB. The committee shall not discuss the issues of AML/CFT against the provision of Section 44 (Ka) of ALPA (regarding information not to be disclosed).
13. The Board shall allocate annual budget and program so that the activities to be performed by the bank in order to prevent the money laundering and financing in terrorist activities on risk-based approach. The committee shall be responsible for preparing a mechanism to ensure its effective implementation and regular monitoring.

2.1.3 AML Committee (Management Level) Responsibilities

AML Management Level committee shall be formed, CEO shall be Coordinator and AML Compliance Officer shall be Member Secretary. Other Members of the Committee shall be decided by the Coordinator of the committee as deemed appropriate. Total numbers of the committee shall not exceed 7 members however any staffs deemed appropriate by the coordinator and/or secretary of the committee shall attend the meeting as invitees.

The AML Committee responsibilities shall be as follows:

1. Review the AML/CFT status of the bank on a regular basis.
2. Ensure that the provisions related to all applicable acts and Directives, Guidelines & Circulars issued by the regulatory authority as well as the internal policies and procedures related to AML CFT are effectively & strictly implemented/complied.

3. Provide recommendation related to AML CFT issues where improvements are needed.

4. Review and discuss the critical observations raised by AML CFT Unit, Internal Audit, External Auditors and Regulators with respect to AML CFT issues.

5. Escalate the critical issues to the ALP Committee for discussion related to AML CFT issues.

2.1.4 Senior Management Responsibilities

2.1.4.1 Chief Executive Officer

Chief Executive Officer is head of the management of the Bank who ensures that the bank has implemented AML/CFT policy and procedure effectively. Following are the main functions 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 best practice 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 taking 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 resources, 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.

2.1.4.2 Senior Deputy Chief Executive Officer (Sr.DCEO), DCEO and Head of the Department

Following are the main responsibilities of Sr.DCEO, DCEO and Head of the Department:

a. Sr. DCEO, DCEO 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 assure that staff 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.

2.1.4.3 Money Laundering Preventions Officer (MLPO)

Chief/Head Legal, Compliance and Governance of the bank shall be the MLPO who would 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 should be sent to FIU immediately.

Bank shall ensure that the appointed MLPO is not a family member or close relative of official of the regulatory authority or high level officials.

In case bank needs to report a suspicious transaction of a customer who is a immediate family member or close relatives of the appointed MLPO, STR shall be reported by an authorized person other than MLPO.

AML/CFT Unit:

The Bank has a separate AML/CFT Unit under MLPO that implements NRB directives, AML ACT/Rules, Bank's AML/CFT policy and Procedures. 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. Manager of AML CFT unit shall also assume responsibility of AML compliance officer who shall ensure an effective implementation of best AML

practices within the Bank and liaise with the central bank for all AML related issues.

Further AML/CFT unit shall review reports issued by auditors, regulatory bodies e.t.c of subsidiaries of NMB Bank to ascertain the compliance with AML/CFT regulation in coordination with NMB Audit team who shall share any non-compliance final findings to AML unit on annual review report. AML unit shall escalate such reports to committees as appropriate.

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.
- As directed by Nepal Rastra Bank.

Responsibilities of MLPO:

- Develop effective policy, procedure and system for the implementation of AML/CFT.
- Review/analyze and send suspicious transaction report to FIU which has been escalated from Department/Unit/Branch.
- Ensure timely reporting of Threshold Transaction Report (TTR) to FIU.
- Consult with other departments or get specialist feedback if needed.
- Prepare the report of the AML/CFT status of the bank.
- Instruct bank's management / all departments for complying the AML Policy, Procedure, NRB Directives etc.
- Make recommendation to take actions to those staff who have not provided required information of paid up capital), Board Members, Top level management and staff. Outsourced resource person may also be used if needed.
- MLPO shall submit the report of AML/CFT status/implementing of/by the bank to ALPC and ALPC shall submit those reports to NMB Board on quarterly basis. NMB Board shall review such report and provide feedback to ALPC or Management accordingly.

- 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.
- 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 ALPC and ALPC shall submit those reports to NMB Board on quarterly basis. NMB Board shall review such report and provide feedback to ALPC or Management accordingly.
- 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 staff. Outsourced resource person may also be used if needed.
- 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 prescribed by regulator.

2.1.5 AML/CFT Officer

Manager - Central Operation, State Service Manager, designated officer of Account Service Operation (ASO) unit and Branch Service Manager of the respective branches shall act as AML/CFT officer. However, AML/CFT officer of respective branch/unit will be primary responsible to implement 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 prescribed under AML/CDD procedure.
e. Send Threshold Transaction Report (TTR) to AML/CFT Unit as prescribed 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 and responsibilities, AML/CFT officers of respective branches/ Department/ Unit 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

2.1.6 Head - Operations

Following are the main responsibilities of Head Operation:

a. To ensure proper implementation of ALPA, its rules, AML policy and procedure.
b. To instruct branch/department to comply the AML/CFT Policy, procedure, NRB Directive, etc.
c. To instruct respective branch/department for rectifying the discrepancies on AML/CFT related matters.
d. To ensure that all accounts 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 respective unit/branch for blocking of account to implement AML policy/procedure.
g. 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 prescribed 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 Human Resource Department for providing training to those staff.
d. Responsible to reasonably assure that staff 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/activities 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 review AML CFT activities as per bank's policy and procedure. 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 under this policy.
c. Internal audit shall independently check and verify the AML Policy and procedure of the bank, ALPA/its rules and NRB Directive at department/ branch/unit and report it accordingly.

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 perspective (criminal activities, sanction list etc.) before recruitment of staff. It is also applicable for outsourced staff.
b. HR shall ensure that the due diligence of all employees is updated regularly and recorded the 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 staff on need basis.
e. HR shall arrange trainings related to AML/CFT to all staff at least once a year. (in the form of e-learning, webinar, class room training as appropriate)
f. HR shall facilitate to provide national and international training on AML/CFT to MLPO, staffs of AML/CFT Unit and any staff who are directly involved in AML/CFT activities.
g. Departmental punishment/action as recommended by MLPO/CEO, shall be taken to those staff who does not comply the NRB directives and AML policy/procedures.

2.1.11 Individual employee

Following are the main role and responsibility of individual employee:

a. Individual employee shall be more vigilant to possible 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 report to the MLPO/AMLPO of the bank.

3. Know Your Customer/ Employee

3.1 Know your customer (KYC):

KYC is the process of verifying the identity of the clients. The term is used to refer to the bank regulation which governs these activities. Documentation of KYC in banks is increasingly demanding for customers to 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 identification document as described 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 described 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 in money laundering or with sanctions list (individual, group and organization) of United Nations (UN), Office of Foreign Assets Control (OFAC), United Kingdom (UK) and European Union (EU). For this purpose, third party data from different international vendor and data from other sources shall be integrated in AML system to identity such customers.

c. In case of power of attorney holder, third party mandate or guarantor in a relationship, such person 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 to be 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 for monitoring high value and suspicious transactions.
d. Establish systems for conducting 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
h. Customer screening

3.3.1 Time line for obtaining KYC

KYC and its supporting documents of the customer can be obtained after establishing a business relationship or doing any transactions in the following cases after approval of Head Operation (HO) or Chief Support Officer & Customer Experience (CSO&CE), support of the respective Chief Business Head (Department Chief) shall be required. The respective business chief shall be responsible for coordinating and obtaining such mission KYC and its supporting document within the prescribe timeline:

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 recommended/desirous for such interruption.
c. If the risk related to money laundering and terrorist financing does not exist with the customer or customer business.

The respective business segment shall ensure that the required KYC document is obtained within a maximum period of one month.

Notwithstanding anything contained in the above, KYC has to be obtained 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 V-KYC (Video-KYC)/Digital Platform

Bank shall also implement the mechanism for conducting know your customer through virtual platform (electronic medium) as V-KYC (Video-KYC) and/or any other digital method as appropriate in order to establish business relationship and deal with customers. There shall be a separate procedure formulated by the management which shall ensure the verification of required documents and information of customers onboard through digital platform on a regular basis. For any update or new process, any potential information security related risks shall be reviewed jointly by Head IT and Head Information Security and probable by Head-Integrated Risk.

3.5 Know your customer for High Risk account

Bank shall ensure whether the customer, beneficial 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 level official/persons or PEPs or customers of foreign organization with high risk category 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 managerial level official of the Bank as per "Operational Authority" must be obtained before establishing business relation or business continuation (account open and review).
b) If the existing customer falls under high risk category, 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 under this category and their transactions.
e) Conduct enhanced customer due diligence (ECDD) of such high risk customer.

3.5.1 Enhanced Customer Due Diligence (ECDD)

Bank shall conduct 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 associates.
d. Customer who makes huge value of transaction, complicated and irrational 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.
f. High risk country.
g. Customer who uses the new technology which is the potential risk for ML/TF.
h. Customer who is suspected for ML/TF/PF.
i. As prescribed by regulator.

3.6 High Net - Worth Individual/Entity

3.6.1 Individual

If any customer maintains deposit balance above NPR 100 million (cumulative of all type of accounts - savings, call, current, fixed etc.) in his/her account that can be withdrawable at any point of time, is classified as high net-worth individual.

3.6.2 Entity

If any customer (non-personal) maintains deposit balance above NPR 200 million (cumulative of all type of accounts - current, call, saving, fixed etc. - excluding loan (loan disburse amount), institutional deposit of such entities, e.g. Government/Semi-government, NTC, NEA, NOC etc.), funds received from the government of Nepal or government – owned organization, in its account that can be withdrawable at any point of time.

3.7 Provisions regarding KYC of existing customers

In case of existing customers maintaining account and/or doing transactions prior to 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.

3.8 Beneficial Owner

Beneficial owner means the ultimate natural person, who owns or controls money or property or customer, 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 makes arrangement. Identity of such beneficial owners must be established in line with the AML CDD Procedure on following conditions:

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

3.9 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)/Proliferation Financing

This policy represents the bank's commitment to preventing risks associated with money laundering (ML), terrorist financing (TF), and proliferation financing (PF). The bank is dedicated to fully complying with the applicable rules and regulations of anti-money laundering and counter-terrorism financing (AML/CFT) in the country. In addition to adhering to the prevailing AML/CFT regulations, the bank also adopts international best practices 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 the policies into the bank and make arrangement to monitor and control risks arising from money laundering, terrorist financing, and proliferation financing activities in daily operations and business transactions. The senior management of the bank shall promote compliance as a core value and culture, ensuring that the bank will not enter into or maintain business relationships associated with excessive ML, TF, or PF risks that cannot be effectively mitigated.

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.

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 conducted 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 authorized body.
e) Bank shall segregate the customers in different category (high, Medium, low) as per their risk level and do the assessment accordingly. Criteria for risk categorization shall be outlined in the AML CDD Procedure.

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 customer's identity vis-à-vis his/her 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/her transactions being considered suspicious or that reporting is underway. The Bank should 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 considering 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. 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 Bank shall implement risk based due diligence procedures that include, but 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 it does 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.

A bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Shell banks may be used to shield the identity of their underlying owners / controllers.

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 (including loan) 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 Politically Exposed 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 objectives 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
c. High risk country/non-cooperative jurisdiction.
d. High cash transactions (including loan proceeds).
e. 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.

Bank shall give special attention to areas which possess comparatively higher risk on the basis of annual AML risk assessment with appropriate amendments/updates in AML CDD procedure.

10. Reporting Related to AML/CFT

When detecting suspicious transaction or having the reasonable grounds to suspect the account transaction 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 submit following report:

- TTR (Threshold Transaction Reports)
- Risk Assessment and review as per annexure 19.4 of NRB Directive 19
- AML CFT Risk Assessment Report
- Offsite data collection (AML CFT Reporting format)
- Bank self-assessment questionnaire (AML CFT Reporting format)

- Annual report of AML/CFT Activities conducted during Fiscal year

11. Provisions regarding restriction in transactions:

Business relationship shall not be maintained or transactions shall not be done in the case of such customers, details shall be described in AML/CDD procedure.

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 his/her authorized staff.

   1. Records of every transaction undertaken for/by a customer must be retained for 7 years.
   2. Account Opening/KYC details of customer, beneficial 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 on suspicious transactions, STR related documents, Wire Transfer related transaction must be retained for 7 years from the date of closure.
   4. Where known that an investigation is going on, the relevant records must be retained until otherwise informed by the authorities to the Bank.

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. However, in case of high level/ranking officials and PEP customers, the records shall be maintained for at least 10 years from the date of his retirement or release from his position.

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's Information

Bank's staff shall not disclose the customer's information (such as report, document, record, account statement and information which are prepared as per the AML/CFT Act, Its' rules and NRB Directive 19) to other customer or any other unauthorized persons. The concerned staff shall take utmost precautions that they do not leak such confidential information. If it is disclosed to any unauthorized, such activity is known as Tipping-Off, that is prohibited by law. Such Tipping-Off shall be 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 frontend services (for dealing with customers), 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.

Special training related to TBML shall also be roll out to relevant staffs every year.

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

14.2 Branches and subsidiary companies

a. Branches in Nepal or any other country and all the subsidiary companies with 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 while 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.

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

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 CDD 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 CEO.

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

- Anti Money Laundering Policy version 7, is here by repealed.
- Activities carried out related to AML monitoring, implementation, reporting etc, under Anti Money Laundering Policy Version 7 shall be considered as done under this policy.