Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) And Know Your Customer (KYC) Policy, 2019

Nepal Bank Limited
Head Office
Kathmandu, Nepal

Contents

ABBREVIATION

AML	Anti-Money Laundering
BO	Beneficial Owner
BOD	Board of Directors
CDD	Customer Due Diligence
CFT	Combating Financing of Terrorism
ECDD	Enhanced Customer Due Diligence
EU	European Union
FIU	Financial Information Unit
HMT	Her Majesty Treasury
KYC	Know Your Customer
ML	Money Laundering
NCDD	Normal Customer Due Diligence
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
RBA	Risk Based Approach
SCDD	Simplified Customer Due Diligence
STR	Suspicious Transaction Report
TF	Terrorist Financing
TTR	Threshold Transaction Report
UN	United Nations

Preamble

Assets (Money) laundering has been an unforgiving problem around the globe. The launderers, Fraudsters and terrorist mainly use banking channel to legitimate their illicit funds and integrate such proceeds into the economy in a way that makes them appear legitimate.

Taking it into account, Nepal bank Limited (NBL) has already promulgated and implemented AML/CFT policy since July 23, 2012 following the norms and sprits of Assets (Money) Laundering Prevention Act 2008 and Nepal Rastra Bank Unified directives. It has also implemented AML prevention procedures since October 25, 2013. With the passage of time, there have been several changes in the regime of AML/CFT and KYC. In the meantime, NRB directive has revealed so many provisions and clauses to be adjusted in the policy following the prevailing Acts, rules and international standards. Accordingly, NBL is going to revise its existing policy and procedures as to AML/ CFT and KYC and brought these documentations in an integrated approach with the name Nepal Bank Limited Anti-Money Laundering (AML) /Combating Financing of Terrorism (CFT) and Know Your Customers (KYC) Policy 2019. To develop this policy, the board of directors has revised this policy and procedural Guidelines in line with the Assets (Money) Laundering Prevention Act 2064, Assets(Money) Laundering Prevention Rules and Directives of Nepal Rastra Bank and FIU-Nepal.

This policy guidelines on AML, CFT and KYC encompass the provisions and guidelines of National laws and international standards for combating of money laundering and financing of terrorism and other provisions as prescribed by Nepal Bank Limited for its applicability.

Chapter-1 General Background

1.1 Introduction to AML/CFT:

For any bank and financial institution, there is a risk of its products and services being used to launder money and finance terrorism. Wealth collected through various predicate offences is brought into financial system with the intention of disguising the original source of wealth. AML/CFT is a strategic mechanism to ensure transparency and stability in financial system to protect broader economy. Its contribution to control financial crime is developing as incredible in the world. The role of banks and financial institution in regard is substantially increasing ever since.

1.1.1 Definitions:

In this Policy, unless the subject or the context otherwise requires,

- The **Bank** shall mean Nepal Bank Limited
- The **Board** shall mean Board of Directors of Nepal Bank Limited.
- **Chairman** shall mean the Chairman of the Board of Directors of Nepal Bank Limited
- **Chief Executive Officer (CEO)** shall mean the person appointed as the Chief Executive Officer of the Bank, appointed by the Board and entrusted with the overall management, administration and operations of the Bank and accountable to the Board.
- **Branch Manager** shall mean the head of branches of the Bank.
- **Department Head** shall mean the head of a particular department of the Bank.
- **Division Head** shall mean the head of a particular division of the Bank.
- **AML/CFT Committee** shall refer to the Board level AML/CFT Committee of the Bank.
- **AML/CFT Management Committee** shall refer to the Management level AML/CFT Committee of the Bank
- **Risk Management Committee** shall refer to the Board Level Risk Management Committee of the Bank.
- **The Policy** shall refer to "Nepal Bank Limited AML/CFT & KYC Policy – 2076 (2019)"
- **Financing of Terrorism:** An act committed by any person who in any manner directly or indirectly and willingly, provides or collects funds, support, or attempts to do so in order to use them by knowing that these funds may be used in whole or in part for the execution of a terrorist act or by a terrorist or terrorist organization.
- **Corresponding Banking:** The provision of banking services provided by one bank (the correspondent bank) to another bank (the respondent bank).
- **Natural Person:** Individual person.
- **Legal Person:** Any company, corporation, proprietorship, partnership firm, cooperatives, or any other body corporate.
- **PEPs:** "PEP" shall mean a politically exposed person. PEPs are individuals who are or have been entrusted with prominent public functions in Nepal and in foreign countries. The term shall also mean the family members and close associates of such persons.
- **Beneficial Owner (BO): BO** shall mean any natural person who, directly or indirectly, owns or controls or directs or influences a customer, an account, or the person on whose behalf a transaction is conducted, or exercises effective control over a legal person or legal arrangement or remains as an ultimate beneficiary or owner of such activities.
- **Customer Due Diligence (CDD)** is a process of identifying a customer trying to maintain a business relationship or has already maintained such relationship or has requested for occasional transactions. It helps the Bank to identify and verify the customers; access and manage risk; develop risk-based, effective and efficient economic control system, and identify

further potential business.

- **Risk Based Approach (RBA)** shall mean the approach of management which focuses on identifying and addressing potential risks of money laundering and terrorism financing.
- **Shell Bank:** it refers to financial institution or group of financial institutions that has no physical existence in the country of incorporation or license or financial institution or group of financial institutions that is not under any regime of effective regulation and supervision.
- Money Laundering (ML): ML is the illegal process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking /commercial transactions. Moreover, it is the process of making illegally-gained proceeds "dirty money" appear legal "clean". Typically it involves three steps: placement, layering and integration.
- **Financing of Terrorism (FT):** It refers to providing finance or financial support to individual terrorist or non-state actors.

1.2 Rationale of AML/CFT-KYC Policy:

Bank is highly committed in to the AML/CFT regime and is in the move to maintain the international standard to address the issue. Bank issues this AML/CFT and KYC Policy 2019 as well as AML/CFT and KYC Procedures-2019. The objective of this policy and procedure is basically designed to adopt Risk Based Approach (RBA) in AML/CFT as well as for effective and efficient implementation of following legal and other persuasive instruments as a general framework against money laundering, financing of terrorism, predicate offences, and other related financial crime.

Bank has been executing AML Policy and Procedures and controlling Money laundering and Terrorism financing activities. It has also been implementing KYC policy through its operation manual part-1, chapter -2.However, some requirements of regulatory provisions driven Banks and Financial Institutions (BFIs) to modify KYC policy with such extended approaches as CDD, ECDD and SCDD so that they could counter ML and TF activities and maintain the stability. In this regards, NBL is practicing AML/CFT and KYC policy in an integrated approach for effective and efficient implementation of following legal and other persuasive instruments as a general framework against money laundering, financing of terrorism, predicate offences, and other related financial frauds such as:

(a) Asset (Money) Laundering Prevention Act, 2064
(b) Asset (Money) Laundering Prevention Rules, 2073
(c) Nepal Rastra Bank, Unified Directives No.19 on AML/CFT to Banking and Financial Institutions,
(d) Nepal Rastra Bank Directives to Money Value Services (money exchange, remittance)
(e) Assets (Money) Laundering Prevention (Freezing of Properties and Funds of Designated Person, Group and Organization) Rules, 2070
(f) Nepal Rastra Bank, Financial Information Unit (FIU) Directives on TTR/STR
(g) Nepal Rastra Bank, FIU Guidelines STR and TTR
(h) Correspondent Bank's requirements in AML/CFT
(i) Related international standards on AML/CFT

1.2.1 Objectives of the AML/CFT and KYC Policy:

The overall objective of AML/CFT and KYC Policy is to establish internal control system regarding assets (Money) laundering prevention activities and the countering the financing of terrorism.

The specific objectives are to:

(a) Develop a sound mechanism for AML/CFT compliance measures as per the requirement of the legal, regulatory and international banking practices.
(b) Adopt Risk Based Approach (RBA) and functionally adequate system controls.
(c) Have a robust customer identification system in line with the effective implementation of KYC and CDD Program.
(d) Develop a mechanism against suspicious transactions and have a stronger monitoring and reporting to the regulatory body as and when necessary.

1.3 Regulatory Requirement:

Bank and financial institutions are required to apply a risk-based approach to identify, assess, monitor, manage and mitigate AML and CFT risks such as:

a) risk management should be based on countries report on national and sectoral risk evaluation,
b) report of any renowned international institutions on AML/CFT,
c) business relationship, nature and transaction threshold.

Bank will classify risk in to high, medium, and low as per regulators direction, international standards, and bank's internal risk based approach and model.

1.4 AML/CFT Compliance Framework:

1.4.1 Formation:

An AML committee is formed with at least one Board member as the coordinator and members including Head, Operation Department (Chief Operating Officer) and Head, Compliance Department as the member secretary. Similarly, more members can be added as per requirements. The committee overviews overall function of the Bank in compliance of the Bank's AML/CFT Policy and Procedures. Similarly, to handle operation issues regarding AML/CFT practice management level committee is formed with Assistant Chief Executive Officer. The CEO / Deputy CEO shall be invited in the meeting.

1.4.2 Implementation Strategies:

The Bank will materialize the objectives of the AML/CFT and KYC policy by the issuance of AML/CFT and KYC Procedures and establishment of necessary operational and system controls. The Bank concentrates on the systematic approach for:

(a) Customer Due Diligence (CDD),
(b) Enhanced Customer Due Diligence (ECDD),
(c) Risk-Based Approach (RBA),
(d) Monitoring and Fraud Detection,
(e) Reporting,
(f) Internal Controls,
(g) Capacity Building,
(h) Review and Appraisal

1.4.3 Action Plan:

The Bank will develop annual plans and programs to implement AML/CFT system and conduct a regular review as well as annual appraisals to ensure the functionalism, its effectiveness, and further

enhancement. To ensure effective implementation of AML/CFT measures, the Bank will implement standard procedures for customer due diligence, risk profiling and management, monitoring, reporting, governance and internal controls, record keeping, human resource management, and training and capacity building.

Chapter-2 Know Your Customer/Customer Due Diligence Policy

2.1 Introduction:

The KYC is the process of identifying and verifying the customers about their identity, address, transactions, profiles based on risk based approach and adopting required measures to protect the bank from being means of money laundering. It is the matter of documented norms for the bank to know legitimacy of its business transactions so as to prevent and control potential risks. It requires due diligence while establishing business relationship. Customer Due Diligence (CDD) is a process of identifying a customer trying to maintain business relationship or has already maintained such relationship or has requested for or already conducted one-off or similar transactions. It is required to identify and verify customers; to assess the risks and manage the risks; to develop risk- based, effective, efficient and economic monitoring system; and to identify further business potential. The CDD process has to be continued to a certain period of time even after such relationship has terminated or transaction has been completed. CDD is a process to review overall activities of a customer and reach to a conclusion. However, bank will take KYC and CDD as per requirement.

2.2 KYC and CDD:

The Bank has following minimum standards set for the KYC/CDD:

(a) No one shall be accepted as a customer or transaction or deal without KYC completed satisfactorily.
(b) No fictitious or anonymous account or transactions or deal will be conducted and no relationship will be established with shell bank or any bank that permits shell bank to have relationships.
(c) Bank shall ensure that Proof of Identity of the person with whom the bank is establishing business relationship or carrying out transaction will be obtained.
(d) Proof of Identity of the person in representative capacity (third party)
(e) Bank shall ensure to obtain power of attorney in required cases to operate bank account or transaction.
(f) Review and update KYC / CDD once a year to those customers who fall in high risk category.

2.2.1 Types of CDD:

Based on different levels of risk, the Bank will adopt following 3 types of CDD.

(a) Simplified CDD - Simplified customer due diligence (SCDD): This can be conducted for customers who fall under low risk customers having characteristics as specified by NRB directive i.e. customers whose identity is publicly available and controlled by national system and other specified by regulator from time to time.
(b) Normal CDD - This is conducted for low risk customers who do not fall under enhanced and simplified customer due diligence.
(c) Enhanced CDD - Enhanced Customer Due Diligence is conducted for high risk and medium risk customers. It refers to the additional due diligence pertaining to the identity of the customer, source of income, nature and value of transaction and others specified by directives.

The Bank can terminate the relationship with the customers or postpone or terminate transaction if they are unable to comply with CDD and consider due examination thereon.

2.3 Customer Identification Process:

Customer identification is an integral part of KYC & CDD process. For the purposes of this policy Customer identification process identifies:

2.3.1 Beneficial ownership:

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

The Bank shall deploy sanction screening programs to safeguard itself from establishing, maintaining relationship or carrying out transaction of a person, group or organization in which a party is sanctioned or directly or indirectly linked to a transaction or is Beneficial Owner (BO) or beneficiary. It shall instigate a control measures for safeguarding the Bank against being used as a conduit for ML, TF and other crimes. For these individuals holding at least the share of 10% or more of ownership intermediate or ultimate holding of the company will be covered.

2.3.2 Politically Exposed Persons (PEPs):

The Bank will develop timely update and maintain the list of high ranking officials and politically exposed persons as per the prevailing Nepali laws and NRB Directives. The Bank will also adopt IT system for identifying, monitoring and managing risks associated with this.

2.3.3 Enhanced Customer Due Diligence (ECDD):

Enhanced Customer Due Diligence (ECDD) process is mandatory for all high risk customers. The Bank aims to reach the reality of the customer and transactions through ECDD process. ECDD includes collection of extensive information of the customer and closely watch on overall activities from different sources. The bank shall apply ECDD to customers who transact via electronic medium, have high net worth, are involved in ML and FT, corruption and tax evasion and are involved in high cash transaction.

2.3.4 KYC for Existing Customers:

Customer Due Diligence Process is also mandatory for all existing customers. The Bank conducts KYC gap analysis in a periodic basis to identify gaps in KYC information then performs CDD of the customers whose mandatory information in the KYC are yet to be recorded.

2.3.5 Walk-in Customer:

Customers that do not have bank account but are taking service from bank by physically presenting themselves in the bank's premises are generally called walk-in-customers. These customers generally come to withdraw money, exchange of currency or to get information. Bank adopts policy of identifying these types of customers depending upon the value of business transaction they perform. In case of customer who has come for withdrawal or exchange of money more than NRs. 100,000, then bank shall conduct due diligence by screening and filling KYC of the customer. In case of business value less than NRs. 100,000, the bank shall get the Identity Proof of the customer.

2.3.6 Non-face-to-face Customer:

For customers performing banking transactions without face-to-face interactions, the bank follows a series of appropriate risk-based policies and procedures to ensure that adequate controls are applied in practice. The type of such procedures required will vary depending upon the nature and scope of the non-face-to-face activities. The extent of verification to be conducted would depend on the nature and characteristics of the product or service requested and bank shall formulate appropriate KYC/CDD.

2.4 Customer Acceptance Procedure:

Bank shall adopt the policy of performing business of different customers by accepting valid and required documents as per banks requirements when customers are on-boarded and renewed. Customers are accepted for establishing business relations and/or providing financial services only after following measures are applied:

(a) Identification of the customer
(b) Verification of customer information
(c) Identification of purpose or objective of business relationship
(d) Obtainment of minimum required documents
(e) Application of risk-based approach
(f) Notification and obtainment of approval
(g) Constructive record keeping

2.5 KYC Review and Update:

Review and update of customer's information is essential and critical to better apply KYC system. The Bank has a system of periodical updating of customer identification data (including photograph/s) after the account is opened or transaction is completed. Bank shall update high risk customers KYC once a year.

Chapter-3 Risk Management Policy

The bank incorporates a Risk- Based Approach (RBA) for the implementation of AML/ CFT measures. It ensures effective CDD program is in place by establishing appropriate procedures and their effective implementation based on risk. It shall also cover proper management, oversight, systems, controls, segregation of duty, training and other related matters. All activities of the Bank will be conducted on risk-based approach. Systematic and scientific methods will be applied for the assessment of risks.

3.1 AML/CFT Risks:

3.1.1 ML/FT Risks:

Use of financial systems for money laundering or financing terrorism creates threat to the state, society and the overall economy. Different vulnerability points such as entry of cash into financial system, cross-border flows of cash, transfer within the financial system, acquisition of investments and other assets, incorporation of companies and formation of trusts are used to launder money. Traders also practice money laundering by using legitimate trade to disguise their criminal proceeds from their unscrupulous sources. Trade Based Money Laundering (TBML) involves a number of schemes in order to complete the documentation of legitimate trade transactions, such actions may include: moving illicit goods, falsifying documents, misrepresenting financial transactions and under-over-invoicing the value of goods. Terrorist groups and organizations may find financial support and conduct revenue generating activities via terrorist financing.

3.1.2 Sanctions Risks:

Sanctions designated individuals and entities pose greater threat of money laundering and terrorist financing. Enrolment of such individuals and entities into the financial system, and delivery for financial services are strictly prohibited.

3.1.3 Customer Risks:

Natural as well as legal persons trying to establish relationship with financial system pose certain level of risk as per their background, occupation, affiliated industry, subscribed products, services, and delivery channels, and transactions. Risk profile of each customer is established while enrolling to the Bank, performing transactions, and other routine operations such as regular profile update, sanction lists update, PEP database update etc.

3.2 Customer Risk Rating policy:

Each customer's profile is rated for different level of risk with respect to the prospects of ML/FT activity. The risk rating is conducted in reference to guidelines recommended by regulatory agencies, international trends in ML/FT activity, national trends, and the bank's internal assessment. For risk assessment customers are to be categorized as high risks, medium risks and low risks. It should be based on factors like: geography, nature of business/ occupation, customer, product, channel, etc. as defined by Risk Based Approach (RBA) Module.

(a) **High Risk:**

- High net worth individuals,
- Customer having transactions with sanctioned countries,
- Customer suspected of ML/FT,
- Proliferation Financing, Arms and Ammunition
- Corruption/Tax Evasion / Revenue evasion

- Narcotic Drugs and psychotropic substances
- Human trafficking/Organized crime/Counterfeiting
- Non face-to-face Customers or Business Transactions
- Cross border correspondent banking
- Wire transfers
- Foreign PEPs, family member and person associated with them
- Casino/Gambling /Bar /Night Club
- Real Estate/ Personal Investment Companies/ Assets management services
- Express Trust/ Remittances/Currency Exchange Transactions/ Virtual Currency Exchanges
- Precious Metal and Gems
- Customers with dubious reputation
- Private banking
- Shell entities/ Shell banks
- Customer under investigation or prosecution or convicted
- Customer with suspected BO
- PEPs, family members and person associated with them,
- Travel agency
- Beauty parlour
- Business of valuables herbs, medicines, ancient items or similar
- Cooperatives
- Customer/ entities having close family share-holding or BO
- Business relation through Internet, Telephone, Fax, Postal service etc.
- Internet Banking, ATM Transaction, Mobile Banking
- Transaction through instruction / request by Fax/wire
- Transaction through Wire or prepaid card, etc.
- Transactions with foreigners and NRNs
- Customer who conducts complex, unusual large transactions and unusual patterns of transactions or with no apparent economic or visible lawful purpose,
- Public servant beyond PEPs and above section officer or equal to that, family member and person associated with them,
- Chief of municipalities, District level and above beyond PEPs
- Members of political parties of district level and above beyond PEPs
- Customer consuming risky products and services,
- INGOs and its affiliates in Nepal
- Trusts/ Charities/ Non-profit organizations receiving donations
- Offshore bank
- Trade Finance especially Letter of Credit
- Pooled accounts/ escrow accounts
- Correspondent bank accounts
- Loan account- NPA
- All other Accounts and transactions which is classified by FIU as high risk account.

All high risks customers shall be treated with the Enhanced Customers Due Diligence (ECDD) exploring the details of their information regarding the transaction, its purpose and source of fund.

Such type of risk customers shall be annually updated and reviewed.

(b) **Medium Risk:**

- Business of non-banking financial institutions,
- Persons with a position to a political party,
- Accounts other than those classified as low risk and high risk.
- Persons engaged in agency works, stock brokers, forex remittance transactions, transactions through alternative channels such as: card, internet banking, mobile banking etc.
- NGOs
- Dormant A/Cs with KYC requirements for activation and fund freezing order
- Transactions related to those entities that are highly regulated/inspected and supervised.

Medium risk customers shall be done with normal customers' due diligence usually called (NCDD) and be reviewed once in every three years.

(c) **Low Risk:**

- Accounts opened for distribution of social security allowances, grants/ reliefs by Government of Nepal,
- Public limited company listed to stock exchange,
- Bank and Financial Institutions licensed by Nepal Rastra Bank,
- Statutory bodies,
- Students/ households, house wife,
- UN Agencies,
- Cottage and small industries, small business,
- School, college, universities,
- Transactions of public enterprises,
- Transactions of Government of Nepal including State and Local Level, Joint Ventures with governments,
- Salaried employees and laborer whose income structure are well defined,
- People from lower economic strata of the society having small balances and low turnover,
- Accounts opened under the program of financial inclusion,
- Transactions of institutions which is established under special Act,
- Facility and incentives provided by Bank and Financial Institutions to their employees.

Low risk customers shall be subject to Simplified Customers Due Diligence and be reviewed as per requirement and change in the regulation or laws.

Customers whose profile matches with sanctions list, adverse media list, or bank's internal black list are assigned with high risk category and any further relationship is terminated immediately. If any customer's profile matches with PEPs or investigation list, the customer's profile is set as high risk profile. Customers are assigned with high risk, medium risk and low risk with respect to their background, occupation, industry, products subscribed, services subscribed, delivery channel subscribed, geographic footprint, and transaction patterns. During the transaction monitoring process, if a customer's transaction pattern is detected to be of high risk, it may trigger for the customer's profile to be escalated to high risk profile.

Bank Compliance Department shall do the necessary risk assessment of the factors that calculates the

risk factors on Risk Based Approach. The factor includes risk weightage of occupation, industries, occupations, bank product and services, geography regions, transaction and different delivery channels offered by bank. The weightage factor is approved by the AML committee and incorporated into bank AML IT system. Such weightage factor is time and again reviewed by bank compliance department and if required are changed on approval from the AML committee of bank.

3.3 Risk Review of Transaction Related to Remittance

Bank is regularly engaged with remittance business .Inward and outward remittance should be assessed by concerned staff and department. Staffs who conduct this business should collect appropriate information and KYC/CDD to know whether the money to be remitted is legal or not. Source and other information's should be collected for the purpose.

3.4 Risk Review of Locker Holders

Locker is provided to the customer who has accounts with the bank. The customer who wants to get this facility must follow the operation procedure as mentioned in operational manual one. Similarly for risk assessment bank should collect KYC/CDD of the customer who has maintained or who is going to maintain accounts. For this purpose the customer availing locker facility should undergo through screening process and will be categorized into low, medium and high risk. PEP and related persons, beneficial owner and related person shall have to be identified and concerned staff should conduct due diligence as it was conducted for opening of other accounts.

3.5 Sanctions Program:

Bank uses United Nations' Sanction List of individuals and entities and OFAC's Specially Designated Nationals list of individuals, entities, cargo, and vessels. Screening against these lists prohibits sanctions designated persons from enrolling into the banking systems as well as restrict further interactions with the bank. Bank shall also use international standard and practices regarding sanction program such as EU, HMT and OFAC etc.

3.6 Transaction Surveillance and Monitoring:

Transaction surveillance and monitoring will be conducted for all customers regardless of the risk rating of their customer profile. Detection of a suspicious activity may result into customer's profile review, update on risk rating and ultimately escalating the customer to higher risk profiles.

Chapter-4 Monitoring Policy

The Bank will ensure a sound monitoring system in place to detect unusual/ suspicious activities/ transactions. Once the customer is on-boarded, monitoring the relationship, transaction, and activity of customer/s will be the major focus of the Bank. Effectiveness of monitoring will also be the target of the compliance, audit, and the management of the Bank.

Automated system will be the primary tool of monitoring. Every transaction will be monitored on a regular basis to revaluation of customer for risk grading and for any suspicious transaction. Staffs at the Bank are required to review the product of monitoring tool and add value to information. Human intervention based monitoring will also be another regular tool for the system.

For effective monitoring, the bank will adopt strategy of regular KYC/CDD update and review mechanism so as to discover ground truth and realistic picture of the business relationship and activities.

4.1 Threshold Transactions:

The Bank follows NRB's recommendation for monitoring threshold transactions. All cash transactions, in-ward and out-ward remittances, and foreign currency exchanges are monitored for whether the transaction value are exceeding the limits defined and instructed by NRB from time to time.

4.2 Suspicious Transactions:

All customers' transaction patterns are monitored for suspicious activities. The patterns of cash transactions, location of transaction, beneficiary, withdrawal from Automatic Teller Machines (ATMs) in Nepal as well as in India, transactions deviating from KYC declaration etc. will be monitored. The Bank regularly updates the scenarios of suspicious activities that may occur as per NRB's guidelines/directives, international practice, and industry standard. The indicators of suspicious transactions shall be cash, funds transfer, economically irrational transactions, behaviours of the customers and miscellaneous grounds for suspicion.

4.3 Customer Profile:

Customers may change their background, occupation, industry, associations, products and services subscribed. Various adverse activities may also occur in relation to the Bank's customers. These changes are reflected into the Bank's AML/CFT measures by regularly monitoring customers' profile as well.

4.4 Lists:

Lists such as sanctions list, PEP lists, adverse media lists, bank's internal black lists etc. will also be monitored against any customer existing and on boarding. Beside international Sanctions list such as UN list, EU list OFAC list and HMT list shall be screened against any customer making cross-border transaction via wire transfer.

Chapter-5 Reporting Policy

Reporting is cardinal organ of AML/CFT regime. The Bank will make optimum focus in identifying, preparing and submitting qualified reports as follows:

(a) **Regulatory Reports**

(i) Regulatory Reports: NRB reports as per Directives,

(ii) FIU Reports: TTR /STR,

(iii) Internal Reports: Various compliance reports and information.

(b) **Other Reports**

Report as per other law enforcement agencies etc.

5.1 Threshold Transaction Reports (TTR):

The Bank shall submit the particulars of transactions following a threshold or in excess of such threshold within 15 days from the date of transaction to the Financial Information Unit (FIU) as per the format prescribed and direction given.

5.2 Suspicious Transaction Reports (STR):

Compliance Officer at the Head office and branch must review the STR flags raised by the AML/CFT system; analyse the transaction and forward for review to Head Compliance Officer (HCO). HCO may override, approve, and reschedule the cases in process of review. Upon approval from HCO the reports of STR shall be sent to financial Information Unit (FIU), NRB.

5.3 Others:

The Bank may also submit other relevant information related to offences and investigations to regulatory body on demand upon request. In general, the bank usually sends the financial information upon the request made by investigation authority, police administration and courts.

Chapter-6 Governance and Internal Control

Bank Board of Directors has constituted an AML/CFT risk committee headed by a board member followed by two members including Head Compliance Officer and Head, Operation Department and other members as deputed to AML Committee by BOD or management. The AML/CFT risk committee is an apex body to have AML regime in NBL. The committee has passed a charter that sets out the terms of reference (TOR) for the AML committee within the provision of prevailing policy guidelines and NRB directives.

6.1 Organization:

The Bank has formed an AML/CFT Committee to coordinate overall AML/CFT activities in the Bank. A Head of AML/CFT that acts as member secretary of the AML/CFT Committee has also been appointed to facilitate the AML/CFT activities. The committee includes;

(a) Board Member- One Coordinator and other members as deputed by BOD
(b) Assistant CEO (Operation Department and / or Compliance Department) - Member
(c) Head Compliance Officer- Member Secretary

6.2 Roles and Responsibilities:

It shall be noted that AML/CFT is responsibility of each and every staff at the Bank. The AML /CFT roles and responsibilities of staff have been already mentioned in existing AML/CFT policy and procedure and shall be provided if special responsibility is to be given to special employee. However, the following staff shall have to play an active role in AML /CFT domain:

(a) Customer Service Desk has primary role of data collection, customer follow-up and record keeping.
(b) Compliance Officers at branches and branch managers shall require monitoring and reporting AML/CFT activities, and facilitate implementation of AML/CFT procedure.
(c) Other Departments including province office shall support compliance department in detecting, identifying and reporting unusual financial and non-compliance activities.
(d) Head Compliance officer shall review AML/CFT activities, report to Chief Executive officer (CEO), AML/CFT risk committee and Board of Directors. Bank management and Board shall ensure availing of resources to the Compliance Officer.
(e) CEO Shall review compliance related Risk and report to BOD.
(f) AML committee shall govern AML/CFT activities of the Bank.
(g) Internal auditors should audit compliance activities in relation to AML/CFT requirements.
(h) BOD reviews compliance as directed by laws, bylaws and NRB Directive and reports to concerns authority.

6.3 Procedure:

The Bank shall develop its AML/CFT procedures as per the guidelines provided by Nepal Rastra Bank, this AML/CFT-KYC policy, and bank's business processes. For critical decision-making in AML/CFT workflows, maker-check verification and proceed with approval mechanisms will be followed. The AML/CFT IT Systems is designed with the same workflow and decision requirements.

Chapter-7 Others

7.1 Record Keeping:

Bank shall keep a record of every transaction, customer data, and data obtained for the purpose of identification, risk analysis, monitoring and other related information along with the date, time and nature, KYC/CDD documents, correspondence with the customers, sources of fund, as well as all documents related to money laundering activities such as files on suspicious activity reports, documentation of AML account monitoring, etc. These records must be kept for a minimum of 5 years until other policy/act is prescribed for more time.

7.2 Human Resource Management:

(a) Bank shall make a proper recruitment and placement policy based on knowledge and skills required to handle AML/CFT and KYC activities

(b) Bank shall provide necessary learning and education schemes to the entire staffsthat are needed to have knowledge to understand and handle AML activities.

(c) Performance evaluation and incentives shall also be linked with the handling of AML, CFT and KYC in the branches and departments.

(d) Regarding employee recruitment and retention of highly disciplined employee bank shall align it with compliance to AML/CFT and incorporate the same into bank HR Policy.

7.3 Training and Awareness:

Bank has been conducting training and orientation programs to all existing as well as newly recruited employees on AML/CFT. All employees (including trainees and temporary personnel) responsible for carrying out transactions and/or for initiating and/or establishing business relationships shall undergo training and orientation. The Bank shall also spread awareness amongst the customers about AML/CFT/KYC measures and the rationale behind them.

Bank shall prepare the annual AML/CFT training calendar. The Compliance Department shall ensure that the training has been provided to the all relevant staff, Board members and stakeholders of the Bank. Bank shall make necessary arrangement for national and international exposure to the concerned staff working and supporting the AML/CFT & KYC regime of bank which should help the staff motivate themselves and gain knowledge from such national and international exposures.

7.4 Technology Adaptation:

Bank shall have an AML/CFT/KYC-friendly new technology in system and interface it with the Core Banking System so that they could perform the entire tasks against the money laundering and terrorism financing and take appropriate measures to prevent the damages to the Bank from its customers. The Bank will ensure that appropriate KYC procedures are duly applied to the customers while using new technology driven products. The AML/CFT and KYC system which are being executed these days in the bank shall help control ML and TF activities with multiple functions such as screening, risk assessment and profiling, transaction monitoring and regulatory reporting. The system shall be made as much flexible as required to integrate with bank's CBS and other software's in future.

7.5 Policy Update:

Bank shall review and update the policy at least once a year and as per requirement.

7.6 Repeal and Savings:

The Nepal Bank Limited AML Policy, 2013 is hereby repealed. All actions taken and functions performed before the commencement of this policy shall be considered to have been taken or performed pursuant to this policy.