AML/CFT Policy and Procedures 2074 (Amended 2079)

RASTRIYA BANIJYA BANK LIMITED

TABLE OF CONTENTS

ABBREVIATIONS

Abbreviations	Full Form
AML	Anti Money Laundering
AOA	Article of Association
BO	Beneficial Owner.
BOD	Board of Directors.
C2B	Call Center to Branch
C2C	Call Center to Customer
CAP	Customer Acceptance Policy
CBS	Core Banking System
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CFT	Combating the Financing Of Terrorism.
ECDD	Enhanced Customer Due Diligence
EU	European Union
FATF	Financial Action Task Force
FCY	Foreign Currency
FDI	Foreign Direct Investment
FIU	Financial Information Unit
FT	Financing of Terrorism
GON	Government of Nepal
HMT	Her Majesty's Treasury
INGO	International Non Governmental Organization
KYC	Know Your Customer
ML	Money Laundering.
MOA	Memorandum of Association
NGO	Non Governmental Organizations
NRB	Nepal Rastra Bank
NRN	Non Resident Nepalese
OFAC	Office of Foreign Asset Control
PAN	Permanent Account Number
PEP	Politically Exposed Person
R- Update	Remote Update
RBA	Risk Based Approach.
RBB	Rastriya Banijya Bank
SAR	Suspicious Activity Reporting
STR	Suspicious Transaction Report
TBML	Trade Based Money Laundering
TTR	Threshold Transaction Report
UBO	Ultimate Beneficial Owner
UN	United Nations

CHAPTER 1

SHORT TITLE, COMMENCEMENT AND DEFINITIONS

1.1. Short Title & Commencement

1.1.1. The policy and procedures set forth herein shall be referred to as "AML/CFT Policy and Procedures 2074 (Amended 2078)".

1.1.2. "AML/CFT Policy and Procedures 2074" of the bank shall provide guidance for designing the anti money laundering and combating financing for terrorism process of Rastriya Banijya Bank. "AML/CFT Policy and Procedures 2074" will be in harmony with the AML/CFT Act 2064, AML/CFT Rules 2073, NRB Directives 2077 and FATF Recommendations.

1.1.3. Approval of the Board of Directors shall be required to amend the provision of "AML/CFT Policy and Procedures 2074".

1.1.4. Where the provisions of the "AML/CFT Policy and Procedures 2074" contradicts with the provisions specified in the Credit Manual, Treasury Manual or any other policy and procedures of the bank, in that case, the provisions specified in the "AML/CFT Policy and Procedures 2074" shall prevail over all other policies to the extent it has bearing on the risk management process of the bank.

1.1.5. "AML/CFT Policy and Procedures 2074" shall come into force from the date of approval of this document by the Board of Directors of Rastriya Banijya Bank Limited.

1.1.6. Considering the factors like ease in implementation and reducing duplication and redundancies, erstwhile separate AML/CFT Policy 2074 and AML/CFT Procedure 2074 has been merged as a single consolidated document as "AML/CFT Policy and Procedures 2074".

1.2. Definitions

Unless otherwise specifically indicated, the following terms used in "AML/CFT Policy Guidelines, 2074 shall have the following meaning(s):

- **The Bank** means Rastriya Banijya Bank Ltd.
- **The Board** means Board of Directors of Rastriya Banijya Bank Ltd.
- **The Chairman** means the Chairman of the Board of Directors of Rastriya Banijya Bank Ltd.
- **The Chief Executive Officer (CEO)** means 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.

- **The Branch Manager** means the head of branches of the Bank.

- **Department Head** means the head of a particular department of the Bank.

- **AML/CFT Committee** refers to the Board level AML/CFT Committee of the Bank.

- **Risk Management Committee** refers to the Board level Risk Management Committee of the Bank.

- **The Policy** refers to "Rastriya Banijya Bank Limited AML/CFT Policy and Procedures-2074"

- **Money Laundering (ML):** Money laundering refers to any of the following acts:

    a) The conversion or transfer of funds, by any person who knows or should have known or there are sufficient grounds for suspecting that such funds are the proceeds of illegal sources, for the purpose of concealing or disguising the illicit origin of such funds or for assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his/her actions.

    b) The concealment or disguising of the true nature, source, location, disposition, movement or ownership of or rights with respect to funds by any person who knows or should have known or suspects that such funds are the proceeds of crime.

    c) The possession, acquisition or use of funds by any person who knows, should have known or there are sufficient grounds for suspecting that that such funds are the proceeds of crime.

- **Financing Terrorism:** An act committed by any person who in any manner directly or indirectly and willingly, provides or collects funds, support, or attempts to do so in order to use them 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.

- **"Act", "Rules" and "Directive":** In this policy, "Act" refers to the Asset (Money) Laundering Prevention Act 2064 and its latest amendment. The "Rules" refers to the Asset (Money) Laundering Prevention Rules 2073 and "Directive" refers to the Directives issued by Nepal Rastra Bank and Financial Information Unit.

- **Terrorist:** Any natural person or organization who commits any of the following acts:

    a) Commits or attempts to commit terrorist acts by any means, directly or indirectly, unlawfully and willfully,
    b) Participates as an accomplice in a terrorist act

c) Organizes or directs others to commit terrorist act or
d) Contributes or cooperates to the group of persons acting with a common purpose of commission of terrorist acts where such contribution or cooperation is made intentionally and with the aim of continuing the terrorist act or with the knowledge or the intention of the group to commit a terrorist act.

- **Corresponding Banking:** The provision of banking services by one financial institution (correspondent bank) to the customer of another financial institution (respondent bank).

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

- **Predicate offence:** Predicate offences in this policy includes following offences.

    a. Revenue evasion,
    b. Organized crime,
    c. Financing of terrorist activities,
    d. Offence under existing law on arms and ammunition,
    e. Offence under existing law on foreign exchange regulation,
    f. Offence under existing law against homicide, theft, fraud, forging of document, counterfeiting, abduction or hostage taking,
    g. Offence under existing law on narcotic drug control,
    h. Offence under existing law on national park and wildlife conservation,
    i. Offence under existing law against human trafficking and transportation,
    j. Offence under existing law on cooperative institution,
    k. Offence under existing law on forest,
    l. Offence under existing law against corruption,
    m. Offence under existing law on bank and financial institution,
    n. Offence under existing law on banking offences and penalty,
    o. Offence under existing law on ancient monument conservation,
    p. Offence under any other law or treaty which Nepal is a party to, as designated by the Government of Nepal through publishing a notice in Nepal Gazette.

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

    a) Establishing business relationship,
    b) Opening of an account,

c) Any deposit or collection, withdrawal, exchange or transfer of funds in any currency or instruments, payment order by electronic or any other means,
d) Use of any type of safe deposit box (locker),
e) Entering/establishing into any fiduciary relationship,
f) Any payment made or received in satisfaction, in whole or in part, of any contractual or other legal obligation,
g) Any payment made or received in respect of a lottery, bet or other game of chance,
h) Establishing or creating a legal person or legal arrangement, or
i) Such any other act as may be designated by the Government of Nepal by publishing a notice in the Nepal Gazette.

- **Legal Person:** Any company, corporation, proprietorship, partnership firm, cooperatives, or any other body corporate.

- **Legal Arrangement:** Trust (express trust) or other similar kind of legal arrangements.

- **Client/ Customer:** Any individual or entity seeking/attempting to enter or has already entered into a business relationship, or conducts a one-off transaction with the bank as principal or as a client/ agent. Any person or entity connected with a financial transaction that may impose significant reputational or other risks to the Bank.

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

- **PEPs:** "PEPs" means politically exposed persons. PEPs are individuals who are or have been entrusted with prominent public functions in Nepal and in foreign countries. At the same time it also includes person who have been entrusted with a prominent function by international organizations, known as International PEP. The term shall also mean the family members and close associates of such persons.

Explanation: Family members include the following types of relationship/s;

i. Grand Parents , Parents and children,
ii. Spouse/partner,
iii. Siblings
iv. In-laws

Close associates include the following types of relationship/s:

i. Partners outside the family unit,
ii. Prominent members of the same political party, civil organization, labor or employee union as the PEP,

iii. Business partners or associates, especially those that share (beneficial) ownership of legal entities with the PEP who are otherwise connected (e.g., through joint membership of a company board),

iv. Anyone who has the sole beneficial ownership of a legal entity which is known to have been set up for the de facto benefit of the PEPs etc.

- **Domestic Politically Exposed Persons (PEPs): Domestic Politically Exposed Persons (PEPs)** means the individuals who are or have been entrusted domestically with prominent public functions. For example The President, Vice-President, Prime Minister, Chief Justice, Speaker of House of Representative, Chairperson of National Assembly, Chief of State, Council of Ministers, Chief Ministers, Members of Federal Legislature, Members of Constitutional Bodies, Speaker of State Assembly, State Council of Ministers, Officers of Special Class or equivalent to Special Class or above Special Class of Government of Nepal, Judges of Supreme Court and High Courts, Deputy Speaker of Provincial Assemblies, Members of Provincial Assemblies, Central Committee Members Of National Level Political Parties, Chiefs And Deputy Chief of District Coordination Committees, Mayors and Deputy Mayors of Metropolitan Cities, Sub Metropolitan Cities And Municipalities, Chairperson and Deputy Chief of Rural Municipalities and Higher Level Office Bearers of Institution partially or fully owned by the Government of Nepal.

- **Foreign Politically Exposed Person: Foreign Politically Exposed Person** means the individuals who are or have been entrusted with prominent public functions by foreign country, for example Head/s of the Nation, Head of the Government, Senior Politician, Central member/s of National level political party, Senior Government, Chief Administrative Officer, Chief Judicial or Military Official, higher level office bearers of State owned Corporations of a foreign country.

- **International Organizations Politically Exposed Person:** It means the persons who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.

- **Beneficial owner: Beneficial owner** means 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.

- **Ultimate Beneficial Owner:** Ultimate Beneficial Owner (UBO) is a natural person who exercises ultimate control over a legal person, entity or an arrangement

- **Customer Due Diligence (CDD):** Customer Due Diligence means the process of identifying and evaluating the customer/s and the assessment of customer risk as a part of know your customer (KYC) process, allowing banks to better identify, manage, and mitigate the AML related risks. The level of due diligence is based on the risk level of the customer and, thus, there may be various levels of due diligence prescribed by the regulator/s or may be decided by the bank itself.

- **Risk Based Approach (RBA): Risk Based Approach (RBA)** means the approach of management which focuses on identifying and addressing potential risks of money laundering and terrorism financing. The core element of this approach is to create the match between "risks and controls" by understanding of the ML/TF risks to which the banks are exposed and apply AML/CFT measures in a manner and to an extent which would ensure mitigation of these risks. There is no universally accepted methodology, which prescribe nature and extent of risk based approach. It provides every bank the flexibility to manage their ML/FT risks in their own way.

- **Suspicious Transaction: Suspicious Transaction/s** means the transaction/s, including an attempted transaction, whether or not made in cash, which to a person acting in good faith;

    - Gives rise to a reasonable ground of suspicion that it may involve proceeds of an offenses specified by the prevailing law/s, regardless of the value involved;
    - Seeks to conceal or disguise the nature or origin of funds derived from illegal activities;
    - Appears to have no any economic rationale or bona-fide purpose;
    - Appears to be in circumstances of unusual, or unjustified complexity;
    - Appears to be deviated from profile, character and financial status;
    - Seems to be made with the purpose of evading the legal and regulatory reporting requirements and
    - Is found to be conducting or supporting the activities relating to terrorism.

- **Suspicious Transaction Report: Suspicious Transaction Report** means the report to be made by Financial Institutions to Financial Information Unit on any suspicious transaction/s or any attempts under the provisions of " Chapter 3, Section7 "dha" of the Asset (Money) Laundering Prevention Act 2064" and point no. 16 of the NRB Directives No. 19.

- **Wire Transfer: Wire Transfer** means any transaction carried out on behalf of an originator (both natural persons and legal entities) through the bank by electronic means with a view to make an amount of money available to a beneficiary at any another BFIs. The originator and the beneficiary may be the same person/s.

- **Financial Information Unit (FIU): Financial Information Unit (FIU)** means the Financial Information Unit (FIU established on April 21, 2008 pursuant to Section 9 of the Assets (Money) Laundering Prevention Act, 2008 within Nepal Rastra Bank (the Central bank) as

an independent unit in order to work against the money laundering and terrorist financing activities. It is the financial intelligence unit of the State of Nepal. It is the central, national agency accountable for receiving, processing, analyzing and disseminating financial information and intelligence on suspicious money laundering and terrorist financing activities.

- **Shell Bank/entity: Shell Bank/entity** means any bank or entity, which has no physical presence in the country in which it is incorporated, licensed or located, and which is not affiliated with a regulated financial services group that is subject to effective consolidated supervision. For the purpose of this clause, presence of local agent or junior level staff does not constitute physical presence. Shell banks/entities in themselves may not be illegal as they may have legitimate business purposes. However, they can also be a main component of underground activities, especially those based in tax havens.

- **Suspicious Activity Reporting (SAR):** SAR means reports submitted by financial institutions to FIU which is based on ML/TF prone activities or behaviors of customers and which does not fall under the category of STR. It shall also mean to include attempted suspicious transactions.

- **Cash Intensive Business (CIB):** Cash intensive business is a business that generates significant portion of its revenue in cash.

- **Multilayered entity:** A multilayered entity is a legal entity which is owned (wholly or partly) by another legal entity at least two layers of holding/ownership chain.

CHAPTER 2

RISK MANAGEMENT FRAMEWORK

2.1. Risk Management Framework

The Bank shall have a strong and effective framework for the management of risk pertaining to money laundering and terrorism financing. Following have been considered as the major pillars of ML/TF risk management framework in RBBL.

2.1.1. Board and senior management oversight: Board and senior management shall conduct oversight function over the ML/TF risk. The mechanism has been specified below.

- Board of Directors shall approve the AML/CFT Policy and Procedures and shall also ensure its periodic update.
- BOD level AML/CFT Committee meeting shall be conducted at least once in every three months. Status update on key activities of Compliance department and progress report on annual compliance program shall be included in the key agendas.
- Board level AML/CFT Committee shall monitor/resolve pending issues (if any) discussed in previous meetings.
- Senior management shall ensure that compliance function is well equipped with necessary logistics and the functions do not suffer due to inadequacy of human resources, both in terms of quantity and competency.

2.1.2. Anti money laundering and reporting system: The bank shall have robust AML & Reporting system. The AML system of the bank shall have features like sanction screening, risk profiling, transaction monitoring, generating red flags/alerts for suspicious transactions, reporting to regulatory body, generating alerts for data update etc.

On the basis of the direction of AML information flow, the reporting system has been categorized as upstream reporting, peer/horizontal reporting and downstream reporting.

Upstream reporting: The flow of information from the Bank to FIU is upstream reporting.

Peer/Horizontal reporting: The flow of information between the departments like treasury, trade finance, credit, compliance and other concerned process owner is peer/horizontal flow of information.

Downstream reporting: The flow of information from compliance department to branches is downstream flow of information. The compliance department provides information in the form of alerts/guidance/circulars to its branches.

The bank shall have robust AML reporting system for the smooth flow of information.

2.1.3. Effective internal control system: As a part of risk management framework, the bank shall ensure that there are sufficient controls in the areas where there is inherent ML/TF risk. Some of the components of internal controls relevant to AML/TF risk are as follows:

- **Risk assessment:** Overall risk assessment shall be conducted once a year and based on that controls are designed.

- **Policy and procedures**: The bank shall ensure that activities performed for AML/CFT like CDD, transaction monitoring, reporting, etc. are guided by AML/CFT Policy and Procedures of the Bank.

- **Segregation of duties and responsibilities**: Segregation of duties and responsibilities is one of the basic and critical components of internal control system. The idea behind this is that no single person is in a position to circumvent controls and remain unnoticed.

- **Appointment of compliance officer**: Compliance Officer shall be appointed as a head of AML/CFT unit and shall fulfill all the duties mentioned in this policy.

- **Reporting**: Board level AML/CFT Committee shall submit a report to Board of Directors regarding compliance and implementation status under AML/CFT Act, Rules, Directives and internal policy of the Bank.

- **Transaction Monitoring**: A separate Standard Operating Procedure shall be developed for suspicious transactions monitoring and reporting.

- **Standardized record keeping**: Records, documents, Information, Report related to AML/CFT shall be kept in a systematic manner.

- **AML/CFT Unit**: AML/CFT unit shall comprise of customer due diligence section, goaml reporting section, transaction monitoring and risk assessment section and correspondent banking section. However, the organization of AML/CFT unit, including the composition of sections can be changed by the head of compliance department after obtaining approval of the AML committee. The AML/CFT unit shall be headed by the compliance officer of the bank.

2.1.4. Internal audit system: The fourth pillar of risk management framework is Internal Audit Function. Internal audit is regarded as third line of defense and is entrusted with the task to independently verify the AML/CFT mechanism of the bank. Bank shall ensure that internal audit function is done at least once a year.

2.2. Risk Management Process

The risk management process consists of identifying risk related to ML/TF, classifying the risk and developing risk based response as below.

2.2.1. Risk Identification

Risk identification is the first step of risk management process. The bank shall identify different parameters for its inherent risk in terms of money laundering and terrorism financing. Some key parameters are mentioned below.

- **Customer:** Customer is someone who establishes relationship with the bank and conducts the transaction. Their wrong intentions reflect on their transactions which ultimately drag the bank into the problem. So the customer shall be identified on the basis of the money laundering /terrorism financing risk they cause to the bank. Some examples are identification of customer based on the industry type they belong, political exposure/power they have, presence of beneficial owner other than the account holder and their involvement in adverse activities.

- **Product and services**: People involved in money laundering and terrorism financing have number of ways to misuse the products and services the bank offer in their favor. So this parameter includes inherent risk on products and services the bank offer to its customers in terms of money laundering and terrorism financing.

- **Country and geography**: All countries and all geographies are not prone to the same level of risk in terms of money laundering and terrorism financing. Like some countries are sanctioned and some geographies are known to be the center of terrorism financing. The bank shall identify the geographical risk in terms of money laundering and terrorism financing for its branches/ transaction/customers.

- **Delivery channel:** In this age of digitalization, BFIs are more inclined towards digital platforms to deliver its products and services. There is always more risk from non face to face customer rather than from the face to face. Thus, the bank shall identify its customers based on the delivery channel.

2.2.2. Risk Classification

After the identification of inherent risk from different parameters, the bank shall categorize these parameters into three level i.e. high risk, medium risk and low risk. The criteria for each of these risks are mentioned below.

High risk category

- Customers whose profiles match to the PEPs, investigation, adverse media list of AML system, grey list as designated by FATF that are duly confirmed by the compliance department.
- Customers who do not fall directly under high risk category at an individual level but whose aggregate risk score (based on different risk criteria) crosses or exceeds threshold high risk score.
- Customers who belong to the following industries
    - Antique dealers (individuals and entities), Jewelers and precious metals,
    - Saving and Credit Cooperatives,
    - Money service bureaus/ Remittance Company /Money Transfer/Money Exchange House,
    - Share broker firm/stock dealer companies,
    - Guthi,
    - Trusts, NGOs, charitable organizations receiving domestic or foreign donations,
    - Cash intensive business,
    - Dealers in arms, Casinos, Bullion dealers including sub dealers &jewelers,
    - Business of precious herbs and medicines,
    - Real estate agents,
    - Unregistered funds.
- High net worth customers:
    - Customer whose annual deposit in saving account is equal to or more than NPR 50.00 mil.
    - Customers who hold prominent position in business, also known as business tycoons and
    - Corporate leaders.
- Customer suspected to be involved in offences related to money laundering and terrorism financing.
- Suspicious transactions/activities reported customers.
- Customer under investigation or prosecution or convicted.

- Customer with suspected beneficial owner other than the account holder.
- A multilayered entity
- Politically exposed persons (PEPs), domestic, international and foreign PEPs, their family member and person associated with them.
- All account of customers domiciled in high risk countries as categorized by FATF and updated by FIU/Home Ministry from time to time.
- FATCA declared customers.
- Customer or transactions related with a jurisdiction fundamentally deficient for the control of following types of crimes in general, but not limited to,:
    - Terrorism and Financing of terrorist activities,
    - Money Laundering
    - Proliferation Financing, Arms and Ammunition
    - Corruption
    - Tax / Revenue evasion
    - Narcotic Drugs and psychotropic substances
    - Human trafficking
    - Organized crime
    - Counterfeiting
- Customer or transactions related with a jurisdiction largely deficient for the control of above listed types of crimes in general or are under a kind of international monitoring
- Non Residence
- Accounts opened through online channel where physical verification is pending.
- Accounts with High value wire transfer
    - Where there is one-time transaction: Amount equal to or above 50 lakhs
    - Cumulative wire transfer in a fiscal year: Amount equal to or above 5 crores

Low risk category

Customers who do not fall under high risk account and

- Accounts of pension holders
- Social security accounts
- BFIs and Sansthan accounts
- People belonging to lower economic strata of the society with actual annual turnover in account less than NPR 1 Lakh.
- All accounts pertaining to the Government of Nepal, Governmental bodies/Corporations/Companies/Organizations, Joint ventures with Government, Regulators, Financial Institutions, and Statutory Bodies.
- Accounts opened under “Kholau Bank KhataAbhiyan 2076” of Government of Nepal.

In case of following cases, the risk category of the customer shall be migrated from low risk to high/medium risk category depending upon the nature of transaction.

- If the customer deposits/transfer fund into the pension holders accounts and social security accounts to the effect that it no longer remains a single way credit account and/or

- If the annual turnover from the account exceeds 1 lakh.

Medium risk category

- All other than those classified as high risk and low risk shall be classified under medium risk category.

2.2.3. Risk Based Response

The Bank shall develop risk based response as below.

- Information Collection: Simplified CDD for low risk, Normal CDD for medium risk and Enhanced CDD for high risk customers/accounts.
- Intensity of Monitoring: Frequent for high risk and less frequent for low/medium risk.
- Reporting: Suspicious transaction reporting for highly suspected accounts, categorizing in watch list for medium risk account and categorizing in closed list for low risk accounts if it does not exhibit strong indicators applicable for suspicious transaction reporting.

A customer shall migrate from low risk category to high/medium risk category if the actual annual turnover from such accounts exceeds NPR one lakh. Bank shall conduct normal/enhanced CDD in all such cases.

2.3. Annual Assessment of ML/FT Risks

The bank shall assess the level of its inherent risk, risk mitigating capability of its control measures and the level of the residual risk using a scientific risk assessment application. For this assessment, risk score and risk weight shall be assigned in a logical manner. Lower the residual risk better is the position of the organization in terms of ML/FT risk. Low inherent risk and strong risk mitigating capability of controls result in low residual risk. Thus the bank shall focus on minimizing the residual risk score by minimizing inherent risk or increasing control effectiveness. It shall be ensured that the residual risk is within the risk appetite of the bank.The bank shall conduct ML/FT risk assessment before the first quarter of every fiscal year. Also, the Bank shall prepare a risk assessment report to verify its assessment and shall submit to regulatory body.

2.3.1. Key Controls

Key Controls are controls over key risks assessed by the Bank. The bank shall have effective control measures in place to minimize the risk of money laundering and terrorism financing. Some examples of controls are transaction monitoring system, CDD process, risk assessment, suspicious transaction reporting, and training and awareness program, sanction/PEP/Adverse

media list management and sanction screening process. The bank shall ensure that people, process and system are working well for the effectiveness of control measures. For example, if suspicious transaction reporting is a control measure, there should be AML system that generates red flags, there should dedicated staffs in compliance department to analyze and report the transaction and there should be a standard operating procedure for such analysis and reporting.

Effectiveness of key controls should be assessed while conducting annual risk assessment and should be modified/enhanced if indicated by the results.

2.4. Product Paper and AML Controls

It shall be ensured that ML/TF risks are identified and assessed in relation to development of new products and new business practices, including new delivery mechanisms, and the use of new technology for both new and pre existing products. The following procedures should be followed in this regard:

a) Bank will conduct proper assessment of ML/TF risks prior to launching a new product, adopting new delivery channel.
b) It shall be the responsibility of the concerned product originating department to consider the risks of money laundering / terrorism financing and conduct product assessment prior to forwarding the proposal for approval.
c) The ML/TF risks of all such product should be assessed and categorized into Low, Medium or High
d) Bank shall launch such products which fall under ML/TF risks of Medium or Low category. However, bank can launch a product with High inherent risk, where appropriate ML/TF controls reduce the residual risk to Medium or Low category.
e) The AML exercise as specified above shall be evidenced and documented in the product papers.
f) The Procedures relating to product paper and AML controls doesn't apply to already existing products at the time of addition of this provision in the AML/CFT policy and procedures of the bank.

CUSTOMER DUE DILIGENCE (CDD)

3.1. Introduction to CDD

Customer Due Diligence (CDD) is a process of identifying and verifying a customer who is trying to maintain business relationship or has already maintained such relationship with the bank. It includes major activities like sanction screening, identifying PEPs and PEPs associates, identifying beneficial owner/ultimate beneficial owner, categorizing the customer under different risk category, conducting ongoing due diligence, monitoring and reporting etc.

Know Your Customer (KYC) is a part of CDD process which is carried out at the beginning of a customer relationship to identify and verify the customer.

3.2. Pillars of Customer Due Diligence

Customer Due Diligence in RBBL is based on following four pillars.

a) Customer Acceptance Policy;
b) Customer Identification and Verification Procedures;
c) Monitoring of Transactions and
d) Risk Management

3.2.1. Customer Acceptance Policy

Bank's Customer Acceptance Policy (CAP) lays down criteria for the acceptance of customer/s. The guidelines in respect to the customer acceptance policy are mentioned below:

- Account shall not be opened in the name altering from the primary identity document, anonymous or fictitious (benami) name(s), blank names or numeric/alphanumeric characters. Theexisting fictitious/anonymous accounts shall be closed immediately.
- Accounts shall be opened only in the name of natural and legal person/organization, the name being the same as in the primary identity document of the person/entity. Accounts may however be opened with different account titles identifying the nature/use/purpose/type of account at the written request of the legal person/organization with appropriate control parameters.
- Minimum required information and documents i.e. proper identification and information pertaining to the prospective client shall be obtained prior to opening account or performing business relation of any kind, as per the AML/CFT Act, AML/CFT Rule, FIU Directives, NRB regulations/Directives and as per the product paper/policy/guidelines set forth by the Bank.
- Necessary checks/ examinations/ verifications shall be made before opening a new account so as to ensure that the identity of the customer does not match with any person

with criminal background or with banned entries such as terrorist individual/s or terrorist organization/s etc.

- When the staff/s designated to open new accounts find sufficient ground/s that the identity of the prospective customer/s could not be verified and/or the prospective customer/s is not disclosing the required identity, the reason for opening account, transaction frequency and volume, etc and any other such information/s deemed necessary for account opening, the staff/s shall defer/refuse to open an account or establish business relationship. The refusal shall be documented properly and shall be communicated to the head of Compliance Department via compliance officer of the branches.
- Further, the Bank shall close an existing account or business relationship under the situation when the designated staff/s is unable to apply appropriate customer due diligence measure/s i.e. unable to verify the identity and/or obtain document/s required as per the risk categorization, due to non-cooperation of the customer or non-reliability of the data /information furnished to the Bank.
- The Bank shall not establish any business relationship/s with the shell companies and the institution/s that deal with shell companies. Any identified business relationship/s with the financial and other institution/s that allow the transaction of shell bank, shall be discontinued. The bank shall not be associated with the entities located in the non-cooperating jurisdictions as identified by the FATF or those sanctioned by the agencies that the Bank refers to like, UN, OFAC, HMT, EU etc.
- Implementation of customer acceptance policy should not be too restrictive resulting into denial of banking services to the general public, especially those who are financially or socially disadvantaged.
- The Bank shall not establish/maintain any relationship with the sanctioned person/entity.
- The decision to open an account of high risk customers including Politically Exposed Persons (PEPs)/family members of PEP and PEP associates shall be approved by a senior management official(Deputy Executive Officer supervising Compliance Department). Information/Documents of such account shall be provided to the Compliance Department.

3.2.2. Customer Identification and Verification Procedures

Customer identification/verification refers to identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information to the Bank's satisfaction and also to satisfy the independent authorities that the due diligence was observed based on the risk profile of the customer in compliance with the existing guidelines in place. The customer identification procedures shall be carried out at the following stages;

- While establishing a banking relationship,
- While opening the account,

- While transferring fund through wire transfers,
- Whenever the Bank feels that it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the accountholder,
- When the bank sells third party products as an agent,
- When high risk customer/s (including politically exposed person/s) conduct each transaction/s,
- When there is suspicion of Money Laundering/Terrorism Financing.
- When the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data and
- Customer identification shall also be carried out in respect of the non-account holders approaching the bank for remittance transaction below one lakh and foreign exchange transaction in cash. At the same time customer identification shall also be done in case of any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Bank.

Following measures shall be applied for customer identification/verification process:

- In case of natural person, obtaining basic information like name, address, date of birth and verifying with the specified legal documents,
- In case of legal entities and legal arrangement, obtaining information about the ownership and control structure of the organization and verifying the same with the specified legal documents,
- In case of the person who works on the behalf of another organization/person, obtaining information along with power of attorney of both person/organization (power of attorney giver and receiver) and
- Obtaining information regarding nature/purpose of business relationship.

3.2.3. Monitoring of Transactions

The Bank shall ensure a sound monitoring system in place to detect unusual/ suspicious activities/ transactions. Once the customer is on-boarded, monitoring the transaction and activity of customer/s shall be the major focus of the Bank.

Transactions monitoring shall be conducted in two phases i.e. from branch level and from compliance department. Branch staff shall review/monitor suspicious transactions on daily basis. In case of high risk customers, each and every transaction shall be closely monitored.

The AML system of the bank shall generate alerts for suspicious transactions using different suspicious transactions rules.

Generally, monitoring shall be conducted for transactions having following features:

a) Transactions beyond KYC declaration,
b) Unusual activities/transactions/behavior,
c) Transaction without or unclear economical/legal objectives,
d) Huge cash transactions,
e) Repetitive under threshold transactions,
f) Other suspicious grounds

3.2.4. Risk Management

The Bank shall have a proper risk management structure comprising of oversight systems, controls, training and other related components for risk management. There shall be a mechanism for identification, measurement monitoring and control for ML/FT risk. At the identification stage, customer shall be categorized into high, medium and low risk category based on ML/FT risk. The ongoing transaction monitoring shall be conducted from branch level and central compliance to re classify the customers under different risk categories. As control mechanism has significant impact on risk management, control tools shall be applied to effectively implement AML/CFT program in the organization.

The ML/FT risk of the bank shall be managed by various authorities in the following manner.

3.2.4.1.Board of Directors

The Board of Directors shall be responsible to approve the AML/CFT policy and procedures. It shall be the responsibility of Board of Directors to address any issues related to policy/procedures. The Board of Directors shall also be responsible for oversight over theAML.TF functions.

3.2.4.2.Senior Management

Senior Management shall be responsible for the implementation of policy and procedures. It shall also be the responsibility to ensure that the bank has all the required procedural guidelines, logistic support and manpower in place to effectively achieve the objectives of this policy.

3.2.4.3.Compliance Department

Compliance Department shall be responsible for overall status monitoring of AML/CFT program. The main responsibility of the compliance department is to monitor the status of AML/CFT policy and procedures implementation and to propel the extent of implementation at branch level.

3.2.4.4.Branches

Branches shall follow the AML/CFT Policy and Procedures of the Bank. At the same time, the branches shall also be responsible to follow the directives, guidelines and instructions provided

by compliance department. Since branch is the first line of defense for ML/FT risk management, it shall be the responsibility of branch to adopt AML/CFT measures effectively and efficiently.

3.3. Customer Due Diligence Steps

Customer due diligence process is described in six steps as below.

3.3.1. First Step: Information Collection, Identification and Verification

- This is the first step of CDD process. During on boarding of the customer, the staff shall collect all mandatory information in Account Opening/KYC form along with a brief interview to identify whether the person is PEPs/ PEP associates or the beneficial owner of the account is other than the accountholder. Bank should obtain information on the purpose and intended nature of the business relationship.
- While identifying the customer, the bank shall obtain the data/information and documents as mentioned below. All the documents and information shall be retained in a legible manner.
- In case the customer does not have the information required in the form, self declaration is required.
- The staff shall then verify the information with the legal documents the customer brings along with KYC form (e.g. citizenship in case of natural person's account). In case such documents are not available, the staffs shall verify the information with other documents (e.g. passport, driving license or voting card). In event where neither citizenship nor passport, driving license or voting card are available, verification can also be done with other documents required by law and practice to ensure that it does not pose higher risks.
- In case there is a multiple layer of ownership and control structure in legal entities/ arrangement or if there is any other person who has control over the legal entities/arrangement then the natural person who has control over the organization shall be identified.
- In case of natural person's account, if transactions are conducted by another person other than the family members i.e. if there is suspected beneficial owner of the account then the beneficial owner shall be identified.
- In case there is cash deposit of more than 1 lakh in any account by any person other than the account holder/operator, identification document along with the purpose of transaction shall be obtained.
- In case of any other occasional transaction by any other person other than account holder/operator, identification document along with the purpose of transaction shall be obtained.

3.3.1.1.Personal Account (In case of Nepalese citizens)

Information required for KYC

i. Intended nature of opening the account
ii. Full legal name, gender, date of birth and nationality
iii. Permanent and current mailing address;
iv. Mailing address of current working organization;
v. Full name of Grand Father, Father, MotherandSpouse (if married);
vi. In case of Nepalese citizen, Citizenship copy or Election voting identification card or driving license or Passport number with issued date, issued place and expiry date;
vii. In case of those Nepalese citizens who have not obtained citizenship certificates, recommendation letter issued by the local government.
viii. In case of Nepalese minor, birth certificate number or minor identification card number with issued date and issuing authority along with the citizenship/passport number of guardian with issued date, expiry date, issuing authority and validity. Once the minor is adult, the account shall be operated by himself / herself with proper documentation.
ix. PAN number (if required)
x. Expected annual income and turnover
xi. Occupation
    a. Name of organization,
    b. Address,
    c. Contact number,
    d. Designation,
    e. Estimated annual income

Documents required

i. Citizenship Certificate (mandatory),
ii. Voter card/License/Passport/PAN card (If further verification is required),
iii. In case of employees working in Government of Nepal, public enterprises and government organization, his/her employee identification card (If citizenship certificate is not available),
iv. In case of teacher, professor, employees of school, college, University funded by GoN, his employee/teacher/professor identification card (If If citizenship certificate is not available),
v. Latest passport size photo
vi. In case of Enhanced CDD, citizenship copies of undivided family members.

KYC/Account opening form to be filled

i. KYC/Account Opening form (Individual/Joint).
ii. Enhanced CDD form (Individual/Joint) if the customer falls under high risk category.

3.3.1.2.Proprietorship/Partnership Account

Information required for KYC/CDD

i. Name of the firm;
ii. Intended nature of opening the account
iii. Detail information of registered address and business address with phone number, email address, website or other mailing address;
iv. Registration certificate, license, certificate to commence business, renewal certificate with issued date, expiry date, issuing authority;
v. Permanent Account Number (PAN) certificate or any other certificate provided by government entity for tax purpose;
vi. Nature of business/transactions;
vii. Scope of work;
viii. Branch offices and places of branch offices;
ix. Estimated annual income and turnover;
x. Personal details of proprietor/partners/account operator and
xi. Other information, if any.

Documents Required

i. Registration Certificate;
ii. PAN Certificate;
iii. Tax clearance certificate or tax deposit certificate of last year;
iv. Audited financial statement of last year;
v. Citizenship certificates of proprietor/ partners/directors/ account operator;
vi. Agreement between the partners if any;
vii. Passport size photographs of proprietor/ partners/directors/ account operator;
viii. Power of attorney to conduct administrative and financial transactions. (in case of partnership firm) and
ix. Any other written agreement if required.

KYC/Account opening form

i. KYC/Account Opening form (Legal Entities) for the firm.
ii. KYC/Account Opening form (Shareholders/Directors/Account Operator) for proprietor/shareholder/director/ account operator / partners.
iii. If the customer falls under high risk category,

- Enhanced CDD form (Individual/Joint) if proprietor/partners/account operator fall under high risk category.
- Enhanced CDD form (Legal Entities) if the firm falls under high risk category.

3.3.1.3.Company Account (Nepalese)

Information required for KYC/CDD

i. Name of the company;
ii. Intended nature of opening the account
iii. Detail information of registered address and business address with phone number, email address, website or other mailing address;
iv. Registration certificate, license, certificate to commence business, renewal certificate with issued date, expiry date, issuing authority and issuing country;
v. Permanent Account Number (PAN) certificate or certificate number provided by government entity for tax purpose;
vi. Nature of business/transactions;
vii. Scope of work;
viii. Branch offices and places of branch offices;
ix. Estimated annual income and turnover;
x. Personal details of members of Board of Directors or Management Committee or such higher level committee if any;
xi. Personal details of shareholders subscribing 10% or more shares of the company;
xii. Personal details of account operator;
xiii. In case 10% or more shares of a company say (A) is held by another legal person say (B) then personal details of shareholders subscribing 10% or more shares of (B) is required;
xiv. If the company is the subsidiary company of foreign company, details (name and address) of parent company and
xv. Other information, if any.

Documents Required

i. Registration Certificate, license, certificate to commence business, renewal certificate
ii. PAN Certificate;
iii. Certificate of Incorporation or Memorandum of Association (MOA) and Article of Association (AOA);
iv. Tax clearance certificate or tax deposit certificate of last year;
v. Audited financial statement of last year;
vi. Board minute mentioning the decision to open and operate the account and authorized person to conduct the transaction;

vii. Power of attorney provided by the board to conduct financial transaction;
viii. Citizenship certificates of Board of directors/ Managing Directors/CEO/Account operator;
ix. Passport size photographs of Board of directors/ Managing Directors/CEO/Account operator and
x. Any other written agreement if required.

Note: Registration certificate is not mandatory for the organizations established under special acts.

KYC/Account opening form

i. KYC/Account Opening form (Legal Entities) for the firm.
ii. KYC/Account Opening form (Shareholders/Directors/Account Operator) for shareholder/director/ account operator.
iii. If the customer falls under high risk category,
    - Enhanced CDD form (Individual/Joint) if the director/shareholder/account operator falls under high risk category.
    - Enhanced CDD form (Legal Entities) if the company falls under high risk category.

3.3.1.4.Club/NGO/Private Public Guthi (Trust Account)

Information required for KYC/CDD

i. Name of the Club/NGO;
ii. Intended nature of opening the account
iii. Detail information of registered address with phone number, email address, website or other mailing address;
iv. Changed address (if registered address is changed);
v. Registration certificate, license, renewal certificate with issued date, expiry date, issuing authority;
vi. Permanent Account Number (PAN) certificate or certificate number provided by government entity for tax purpose;
vii. Nature of transaction;
viii. Scope of work;
ix. Branch offices and places of branch offices;
x. Estimated annual income and turnover;
xi. Personal details of managing director/account operator/trustee/controller/protector/settler;
xii. Other information, if any.

Documents Required

i. Registration Certificate, license, renewal certificate;
ii. PAN Certificate;
iii. Constitution, Bye Rule as per the nature of the institutions;
iv. Tax clearance certificate or tax deposit certificate of last year;
v. Audited financial statement of last year;
vi. Minute of Working Committee for account opening;
vii. Authority to operate the account and financial transaction;
viii. Citizenship certificates of managing director/account operator,
ix. Passport size photographs of managing director / account operator and
x. Any other written agreement if required.

KYC/Account opening form

i. KYC/Account Opening form (Legal Entities) for the Club/NGO.
ii. KYC/Account Opening form (Shareholders/Directors/Account Operator) for CEO/account operator/trustee/controller/protector/settler.
iii. If the customer falls under high risk category,
    - Enhanced CDD form (Individual/Joint) if managing director/account operator/trustee/controller/protector/settler falls under high risk category.
    - Enhanced CDD form (Legal Entities) if the Club/NGO falls under high risk category.

3.3.1.5.Account for Cooperatives

Information required for KYC/CDD

i. Name of the cooperative;
ii. Intended nature of opening the account
iii. Detail information of registered address and business address with phone number, email address, website or other mailing address, if any;
iv. Registration certificate, license, certificate to commence business, renewal certificate with issued date, expiry date, issuing authority;
v. Permanent Account Number (PAN) certificate or certificate number provided by government entity for tax purpose;
vi. Nature of business/transaction;
vii. Scope of work;
viii. Branch offices and places of branch offices;
ix. Estimated annual income and turnover;
x. Personal details of Board of Directors/ Managing Director/CEO/Account Operators and

xi. Other information, if any.

Documents Required

i. Registration Certificate/ license/certificate to commence business/renewal certificate;
ii. PAN Certificate;
iii. AOA, MOA, Bye Rule;
iv. Tax clearance certificate or tax deposit certificate of last year;
v. Audited financial statement of last year;
vi. Board minute mentioning the decision to open and operate the account and authorized person to conduct the transaction;
vii. Power of attorney provided by the board of directors to conduct financial transaction;
viii. Citizenship certificates of CEO/ board of directors/ account operator;
ix. Passport size photographs of CEO/ board of directors/account operator.
x. Other documents if any.

KYC/Account opening form

i. KYC/Account Opening form (Legal Entities) for Cooperatives.
ii. KYC/Account Opening form (Shareholders/Directors/Account Operator) for CEO/directors/account operator.
iii. If the customer falls under high risk category,
    - Enhanced CDD form (Individual/Joint) if managing directors/ board of directors/ account operator falls under high risk category.
    - Enhanced CDD form (Legal Entities) if the Club/NGO falls under high risk category.

3.3.1.6.Account for Public/Private Guthis

Information required for KYC/CDD

i. Name of the Guthi legal arrangement;
ii. Detail information of registered address with phone number, email address, website or other mailing address;
iii. Changed address (if registered address is changed);
iv. Registration certificate, license, certificate to commence business, renewal certificate with issued date, expiry date, issuing authority;
v. Approval certificate or License and approval letter for transaction, renewal certificate, date of issue, validity and issuing authority;
vi. Permanent Account Number or such certificate issued by government entity for taxation purpose;
vii. Nature of business/transaction;
viii. Scope of work;

ix. Branch offices and places of branch offices;
x. Estimated annual income and turnover;
xi. Personal details of Board ofDirectors/Members of Management Committee or any other committee/managing director/ account operator and
xii. Other information, if any.

Documents Required

i. Registration Certificate, license, renewal certificate;
ii. PAN Certificate;
iii. Constitution;
iv. Tax clearance certificate or tax deposit certificate of last year;
v. Audited financial statement of last year;
vi. Kabuliyatnama regarding the establishment of Guthi;
vii. Board/Management Committee minute mentioning the decision to open and operate the account and authorized person to conduct the transaction;
viii. Power of attorney provided by the Board of Directors/Management Committee to conduct financial transaction;
ix. Citizenship certificates of managing director/ board of directors/ account operator;
x. Passport size photographs of managing director/ board of directors/ account operator and
xi. Other agreements/documents if any.

KYC/Account opening form

i. KYC/Account Opening form (Legal Entities) for Cooperatives.
ii. KYC/Account Opening form (Shareholders/Directors/Account Operator) for CEO/directors/account operator.
iii. If the customer falls under high risk category,
    - Enhanced CDD form (Individual/Joint) if managing director/ board of directors/ account operator falls under high risk category.
    - Enhanced CDD form (Legal Entities) if the Club/NGO falls under high risk category.

3.3.1.7.Account for School/College/Campus

Information required for KYC/CDD

i. Name of the school/campus;
ii. Detail information of registered address and with phone number, email address, website or other mailing address;
iii. Changed address (if registered address is changed);
iv. Registration certificate with registration number, issued date and issuing authority;

v. Permanent Account Number (PAN) certificate or certificate number provided by government entity for tax purpose;
vi. Nature of business/transaction;
vii. Scope of work;
viii. Branch offices and places of branch offices;
ix. Estimated annual income and turnover;
x. Personal details of Managing Director/Board of Directors/members of Management Committee or such higher level committee if any and
xi. Personal details of account operator.
xii. Other information, if any.

Documents Required

i. Registration Certificate;
ii. Approval Certificate;
iii. PAN Certificate;
iv. Certificate of Incorporation or Memorandum of Association (MOA) and Article of Association (AOA);
v. Tax clearance certificate or tax deposit certificate of last year;
vi. Audited financial statement of last year;
vii. Board minute mentioning the decision to open and operate the account and authorized person to conduct the transaction;
viii. Power of attorney provided by the board to conduct financial transaction;
ix. Citizenship certificates of managing directors/ board of directors/account operator;
x. Passport size photographs of managing directors/ board of directors/account operator and
xi. Other agreements/documents if any.

KYC/Account opening form

i. KYC/Account Opening form (Legal Entities) for the school/campus.
ii. KYC/Account Opening form (Shareholders/Directors/Account Operator) for director/ CEO/account operator.
iii. If the customer falls under high risk category,
    - Enhanced CDD form (Individual/Joint) if managing directors/ board of directors/account operator operator falls under high risk category.
    - Enhanced CDD form (Legal Entities) if the company falls under high risk category.

3.3.1.8.Account for INGOs

Information required for KYC/CDD

i. Name of the organization;
ii. Detail information of registered address with phone number, email address, website or other mailing address, if any;
iii. Registration certificate (with registration number, registered office and date);
iv. Permanent Account Number (PAN) certificate or certificate number provided by government entity for tax purpose;
v. Nature of transaction;
vi. Scope of work;
vii. Branch offices and places of branch offices;
viii. Estimated annual income and turnover;
ix. Personal details of board of director/managing director/account operator/representative for Nepal and
x. Other information, if any.

Documents Required

i. Registration Certificate, license, renewal certificate;
ii. PAN Certificate;
iii. Constitution of the organization;
iv. Tax clearance certificate or tax deposit certificate of last year (if required);
v. Audited financial statement of last year;
vi. Agreement if any between the organization and social welfare council of Nepal;
vii. Agreement if any between the organization and GoN;
viii. Reference letter from concerned country or embassy of the concerned country (Not applicable if the organization has taken affiliation from government entity);
ix. Minute of Working Committee for account opening;
x. Authority to operate the account and financial transaction.
xi. Citizenship certificate/passportof board of director/managing director/ representative for Nepal/account operator,
xii. Passport size photographs of board of director/managing director/ representative for Nepal/account operator,
xiii. Any other written agreement if required.

KYC/Account opening form

i. KYC/Account Opening form (Legal Entities) for the INGO.
ii. KYC/Account Opening form (Shareholders/Directors/Account Operator) for board of director/managing director/ representative for Nepal/account operator,
    - If the customer falls under high risk category, Enhanced CDD form (Individual/Joint) if board of director/managing director/ representative for Nepal/account operator falls under high risk category.
    - Enhanced CDD form (Legal Entities) if the INGO falls under high risk category.

3.3.1.9.Personal Account (In case of Foreign Nationals)

Information required for KYC

i. Full legal name, gender, date of birth and nationality;
ii. Permanent and temporary address in foreign country;
iii. Address in Nepal;
iv. Details of family members;
v. Passport number with issued date, issued place, issued country and expiry date;
vi. Visa expiry date;
vii. In case of employee, name, address, contact number and recommendation letter of current working organization;
viii. In case of Indian citizens who do not have passport, legal certificate verifying Indian citizenship with certificate number, issued date, issuing authority and place and also Embassy letter (if available);
ix. In case of the refugee, identity card issued by government or international authorities with identity number, issued and expiry date and issued place;
x. Estimated income and turnover and
xi. Other information, if any.

Documents required

i. Passport;
ii. Visa;
iii. Latest passport size photo;
iv. In case of Indian citizens who do not have passport legal certificate verifying Indian citizen and embassy letter (if available);
v. In case of Enhanced CDD, citizenship copy of undivided family members;
vi. In case of the refugee, identity card issued by government or international authorities and
vii. In case of employee, recommendation letter of current working organization;

KYC/Account opening Form to be filled

i. KYC/Account Opening form (Individual/Joint).
ii. Enhanced CDD form (Individual/Joint) if the customer falls under high risk category.

3.3.1.10. Company Account (Foreign)

Information required for KYC/CDD

i. Name of the company;
ii. Detail information (Country/Province, City, Street, House No., phone number, email address, website or other mailing address) of registered address and business address in foreign country;
iii. Detail information of representative office in Nepal;
iv. Type of office in Nepal (Branch office/ contact office/project office or any other);
v. Registration certificate, license, certificate to commence business, renewal certificate with issued date, expiry date, issuing authority at foreign country;
vi. In case of the companies registered in Nepal, registration certificate, license, certificate to commence business, renewal certificate with issued date, expiry date, issuing authority ;
vii. Nature of business/transaction;
viii. Scope of work;
ix. Branch offices and places of branch offices;
x. Estimated annual income and turnover;
xi. Personal details of Board of Directors/Managing Director of foreign company;
xii. Personal details of account operator and representative for Nepal;
xiii. Other information, if any.

Documents Required

i. Registration Certificate, license, certificate to commence business, renewal certificate;
ii. Certificate of Incorporation or Memorandum of Association (MOA) and Article of Association (AOA);
iii. Tax clearance certificate or tax deposit certificate of last year;
iv. Audited financial statement of last year;
v. Power of attorney provided by foreign company to open the account and conduct financial transactions;
vi. Citizenship certificates/Passport of main Board of directors/ Managing Directors/Account operator/Representative of Nepal;
vii. Passport size photographs of Board of directors/ Managing Directors/Representative for Nepal/Account operator;
viii. Any other document/written agreement if required.

KYC/Account opening form

i. KYC/Account Opening form (Legal Entities) for the company.
ii. KYC/Account Opening form (Shareholders/Directors/Account Operator) for board of directors/managing /director/ account operator / representative of Nepal.
iii. If the customer falls under high risk category,
    - Enhanced CDD form (Individual/Joint) if board of directors/managing /director/ account operator / representative of Nepal falls under high risk category.
    - Enhanced CDD form (Legal Entities) if the company falls under high risk category.

3.3.1.11. Account for Diplomatic Mission/Embassy

Information required for KYC/CDD

i. Name/address of embassy;
ii. Letter from Embassy/Diplomatic mission;
iii. Personal details of account operator and
iv. Other information, if any.

Documents Required

i. Letter from Embassy/Diplomatic mission;
ii. Power of attorney to operate the account;
iii. Citizenship/Passport of account operator;
iv. Passport size photographs of account operator and
v. Other documents if any.

KYC/Account Opening form (Legal Entities) for the firm,

i. KYC/Account Opening form (Shareholders/Directors/Account Operator) for board of directors/managing /director/ account operator / representative of Nepal.
ii. If the customer falls under high risk category,
    a. Enhanced CDD form (Individual/Joint) if board of directors/managing /director/ account operator / representative of Nepal falls under high risk category.

3.3.1.12. Account for Non Resident Nepalese

Information required for KYC/CDD

i. Full name;
ii. Nationality, gender, date of birth;

iii. Full address in foreign country (Country/Province, City, Street, House No., phone number, email address, website or other mailing address, if any) NRN code and details of contact person in Nepal;
iv. Full address in Nepal;
v. Family details (Name of grandfather, father, mother, spouse (if married) and
vi. Other information, if any.

Documents Required

i. Passport certificate with issued date, validity, expiry;
ii. Documents of source of income;
iii. NRN certificate issued by concerned authority of GoN;
iv. Passport size photographs and
v. Other document if any.

KYC/Account opening form to be filled

i. KYC/Account Opening form (Individual/Joint).
ii. Enhanced CDD form (Individual/Joint) if the customer falls under high risk category.

3.3.1.13. Account for Consumer Committee

Information required for KYC/CDD

i. Letter issued by concerned consumer committee regarding the decision to constitute the consumer committee andoperate the account;
ii. Recommendation letter along with the name of account operator issued by local government to operate the account;
iii. Nature of transaction;
iv. Expected annual turnover from the account;
v. Registration certificate number, issued date and issuing authority (if any);
vi. Personal details of members of consumer committee /account operator,
vii. Self declaration of the consumer committee to operate the account as per the purpose of constitution of consumer committee and
viii. Other information, if any.

Documents Required

i. Letter issued by concerned consumer committee regarding the decision to constitute the consumer committee andoperate the account;
ii. Recommendation letter along with the name of account operator issued by local government to operate the account;
iii. Citizenship certificates of members of consumer committee /account operator;

iv. Registration certificate if registered under any government entity;
v. Passport size photographs of account operator;
vi. Self declaration of the consumer committee to operate the account as per the purpose of constitution of consumer committee and
vii. Other information, if any.

KYC/Account opening form to be filled

i. KYC/Account Opening form (Legal Entities) for the consumer committee.
ii. KYC/Account Opening form (Shareholders/Directors/Account Operator) for members of committee/account operator
iii. Enhanced CDD form (Individual/Joint) if members of consumer committee/account operator falls under high risk category

Accounts can be opened in the name of local consumer committees which are registered with concerned government authority and recommended by local body. Such accounts can be opened after taking KYC information of office bearers /members/account operators of such committee upon condition that accounts operators will be responsible on transactions in such accounts.

3.3.1.14. GoN, Offices/Entities established under GoN, Entities established under Special Act, Enterprises under government ownership, BFIs licensed by Nepal Rastra Bank, Insurance companies licensed by Insurance Board, United Nations or offices/entities under UN, International Organizations and Foreign Embassies

Information required for KYC/CDD

i. Personal details of account operator;
ii. In case any permanent employee of GoN has to operate the account on the behalf of the GoN, Identity card of office.
iii. Other information, if any.

KYC/Account opening form to be filled

i. KYC/Account Opening form (Legal Entities),
ii. KYC/Account Opening form (Shareholders/Directors/Account Operator) for account operator
iii. Enhanced CDD form (Individual/Joint) if account operator falls under high risk category

3.3.2. Second Step: Customer Screening

- Screening the customer against sanction lists, PEP list, adverse media list and other list is a very important step in customer due diligence process. During this process, the staff enters the basic information of customer (e.g. name, address, identification no.)into the

AML system and such information are screened against the data maintained under sanction lists (UN, OFAC, EU and HMT), PEP list, adverse media list and other list (Internal investigation list and negative list) of AML system to ascertain whether a customer or related person or beneficial owner falls under such list or not.

- In case of name match, the screening employee should further ascertain whether the address also matches or not. Where both the name and address gets matched with the list, it shall be the duty of branch management to consult with the central compliance team for appropriate guidance and based on that the branch official shall act accordingly.
- In case the name of the customer or his/her family members or nominee of that person matches under PEP list, the employee entrusted with the screening function should carry out adequate due diligence to ensure whether the match is accurate or not. Further, the employee should verify whether the name, address and office information of the customer also matches with the list or not. If all these information are100% matched, the concerned staff shall categorize the customer under high risk category and conduct enhanced due diligence.
- In case the customer or his/her family members or nominee of that person does not match under any PEP list but the staff has unconfirmed reason to believe that the person is PEP or associated with PEP, then in that case also the customer shall be considered as potential PEP and categorized under high risk category.
- Prior approval of senior management is mandatory before opening the account or before establishing any kind of relationship with PEPs and PEPs Associates.

3.3.3. Third step: Risk Profiling

Risk profiling is a process of classifying the customers under different risk category in terms of money laundering and terrorism financing risk. The extent of ongoing due diligence including re classification of customers, monitoring and reporting shall be done according to the risk category of the customers. Risk profiling shall be done in two stages as below.

- **First Stage**: At the time of account opening, branches shall categorize the customer under high/medium/low risk category based on the screening result, information provided by the customer in account opening form and subjective judgment of the staffs which is documented in account opening form.

- **Second Stage**: In second stage, branches shall update KYC information in the AML system. The system then assigns a risk value to the customer based on the different parameters like initial screening result, occupation, geography, product type, channel of distribution etc. The customer shall be categorized under high risk, medium risk or low risk accordingly.

3.3.4. Fourth Step: Account Opening

After risk profiling of the customers, account opening process shall start in core banking system. Employees responsible for account opening shall ensure that all the mandatory fields of core banking system are filled while opening the account and same shall be updated in AML system. Keeping all the records and documents of customer intact shall also be the responsibility of branches.

3.3.5. Fifth Step: Ongoing Due Diligence

- Ongoing due diligence is the process of monitoring the transactions of customers after opening the account. The main objective of ongoing due diligence is to verify if the transaction matches/conforms to the profile of the customers.

- Risk based approach shall be applied while conducting customer due diligence i.e. Simplified CDD for low risk customers, Normal CDD for medium risk customers and Enhanced CDD for high risk customers. However, a customer shall migrate from low risk category to high/medium risk category if the actual annual turnover from such accounts exceeds NPR one lakh. Bank shall conduct normal/enhanced CDD in all such migrated cases.

- Enhanced customer due diligence is required for customers who fall under high risk category. For this, the branch staff shall request the customer to fill up the enhanced due diligence form and retain the same. It shall be the responsibility of branch management to provide the details of such customer to compliance department on a quarterly basis.

3.3.6. Sixth Step: Reporting

In case of any suspicious transaction or activities, the branch staff shall immediately inform the compliance department via filled STR form or email. It shall be the responsibility of branch management to ensure that information pertaining to STR is not disclosed to any other person. Notable is the fact that tipping off is considered as a serious offence as per prevailing act of the country. Normally CDD procedures should be completed before filing any STR/SAR with FIU. However, where completion of CDD procedures could lead to tipping off, bank shall consider filing SAR/STR pending completion of CDD.

3.4. Risk Based Approach to CDD

3.4.1. Simplified CDD

Simplified CDD refers to obtaining minimum information from the customers while opening the account or updating the KYC information. It shall be applied to those customers who falls under low risk category as mentioned in this policy. However, a customer shall migrate from low risk

category to high/medium risk category if the actual annual turnover from such accounts exceeds NPR one lakh. Bank shall conduct normal/enhanced CDD in all such migrated cases. Also, the Simplified CDD measures do not apply when there is suspicion of ML/TF, or specific higher risk scenarios apply.

It shall be noted that simplified CDD shall not be valid if the customer's profile migrates from the low risk category to other categories like high risk or medium risk. The risk category of the customer shall be reviewed / updated on two bases. First one is periodic basis and second one is trigger basis. In periodic basis, KYC information is updated in every five years for low risk category. However, if there are changes in KYC information/transactions, customer due diligence procedures shall be applied based on the appropriate risk category. Simplified CDD form shall be used to obtain KYC information under this approach.

3.4.2. Enhanced Customer Due Diligence (ECDD)

Enhanced CDD refers to obtaining additional information of the customer while opening the account or updating the KYC information. Additional information includes details of occupation/business, source of fund, source of net worth, statements/documents as evidence etc.

Following customers shall be eligible for ECDD

- Customers who are categorized under high risk category during initial screening process in AML system i.e. PEPs, Family members of PEP and PEP associates.
- Accounts having beneficial owner other than the account holder.
- Customer having high risk score in AML system.
- Customers who match the high risk category list as mentioned in this policy.
- Customers who conduct high volume and complex transactions with unclear economic and business purpose.
- Customers who uses high risky new product or services of the bank as notified by the compliance department.
- Customers who are suspected of committing offences under money laundering and terrorism financing.
- Customers of those countries which are internationally identified for not complying or partially complying the international guideline related to AML/CFT.
- Customers having high net worth.
- Customers who conduct large and suspicious transactions systematically via electronic means.
- Customers who are involved in cash intensive business.
- Customers who are convicted from the court for being involved in activities/offences those are unethical as per the prevailing law.
- Natural and legal person belonging to Jurisdictions that are under increased monitoring by FATF.

Following actions shall be taken while conducting Enhanced Customer Due Diligence

- While establishing business relationship with above mentioned customers, following activities should be done
    - Obtain additional information like details of occupation, personal and family background, source of wealth, source of fund, nature/purpose of transactions and beneficial owner information and same should be documented by way of ECDD form.
    - Ask the customer to provide documents as an evidence of information furnished if possible like PAN certificate, Tax clearance certificate, bank statement, audited financial statement (in case of legal entities).
    - Verify the information and documents provided by the clients applying appropriate measures.
    - Keep the form and documents intact and send the scanned copy of ECDD form to compliance department.

- In each and every step of transaction conducted by above mentioned customers
    - Identify and verify the source of transactions that are complex, huge and unnatural in nature.
    - Obtain information or evidence of the purpose of the transactions.
    - Determine the limit of the transaction for ongoing monitoring.
    - Identify if there is any beneficial owner other than the account holder.
    - Obtain/analyze additional information like professional relationship of the customer, nature of transaction and customer's customer.

- The concerned branch compliance officer shall fill up (enhanced customer due diligence internal observation form) to incorporate quantitative analysis (transaction based) for high risk accounts at least once a year.

- It shall be noted that if any suspicion arises while conducting the procedures as mentioned above, the branch management shall fill up the STR form and send to the compliance department.

- It shall be the duty of branch management to ascertain the nature and intensity of additional risk that the bank faces by establishing business relationship with such customers which shall be facilitated by the enhanced customer due diligence exercise.

3.4.3. Standard/Normal Customer Due Diligence

Standard/Normal customer due diligence refers to the due diligence process that is applied for all customers who fall under medium risk category. Customers who do not fall under the high and low risk category are considered as medium risk customers.

The entire information obtained from the customer during the standard customer due diligence process should be documented by way of standard customer due diligence form. Branch operation department of the bank shall ensure that the different forms are being used by branches appropriately based on the risk category of the customer.

3.5. Linking of Accounts

Linking accounts refers to the process whereby accounts opened in CBS are linked to the AML system of bank. It shall be the duty of branch management to ensure that all the accounts are linked to the AML system. Failure to link accounts to AML system might result in underreporting of TTR, STR and customer accounts to regulatory authority for which branch management shall be answerable.

3.6. Provisions Relating to Accounts Opened Through Online Channel

The following provisions shall be taken into account regarding online account opening:

- The bank shall ensure that the customer identification along with his/her geolocation is verified before opening account via online channel.
- The bank shall consider ML/TF risks before introducing the mechanism of online account opening.
- The incremental risk to which bank is exposed should be within the ML/TF risk appetite as set by the board.
- All such accounts shall be debit restricted unless the customer visits the concerned bank and complete the verification mechanism.
- Customers who open account through online channel whose physical verification is pending should be considered as non face to face customer and treated as high risk customers.
- Branch shall monitor the transactions in such account in an extensive manner and any suspicion shall be reported to the compliance department for STR reporting.

3.7. Provisions Regarding Screening Mechanism of respondent Banks

The Bank shall adopt following measures while conducting cross-border corresponding relationship.

- Screening the name/address of the respondent bank to ensure that the bank does not fall under any sanction list or FATF designated countries.
- Conducting proper due diligence of the respondent bank
    - To identify and verify the identification of the respondent bank
    - To obtain business information of the respondent bank.
    - To ensure that the bank is not shell bank and the bank is not allowing any shell bank to use its account.
- Obtaining following documents of respondent bank
    - Board member details along with their National Id card or citizenship certificate.
    - Ownership structure.
    - Wolfsberg questionnaire duly filled up.
    - FATCA Renewal form/ W-8BEN-E form.
    - US patriot act certificate.
    - Memorandum of Association, Articles of Association, Banking License, Registration documents.
- Monitoring suspicious transactions of respondent bank and if any suspicion found, reporting to FIU, Nepal.

3.8. Subsidiary Company AML Process

The subsidiary companies of the bank shall also adhere to appropriate norms relating to AML/CFT. The Board and AML committee of the bank will discuss the robustness of such process of subsidiary companies on a periodic basis.

3.9. Special Provisions Relating to Wire Transfers

Wire transfer poses high risk of money laundering and terrorism financing to the country. In order to minimize this risk the bank should obtain required information related to originator and beneficiary involved in wire transfer such as

- the name of originator/beneficiary,
- address of originator/beneficiary,
- the originator account number where such an account is used to process transaction or in absence of an account, a unique transaction reference number which permits traceability of transaction,
- the beneficiary account number where such account is used to process such transaction or in absence of account, citizenship details of the beneficiary in case of transaction below Rs. 1 lakh.

- Purpose of transaction.

In case of high value wire transfer (equal to or above NPR 50 lakhs), the Bank shall adopt following measures:

- The concerned processing department shall ensure that following information/documents are obtained from concerned branch office before approving the high value wire transfer.
    - Nature/purpose of transaction
    - Source of transaction
    - Relationship between the originator and the beneficiary
    - Supporting documents to verify the transaction
- The compliance department shall monitor high value wire transfers on a quarterly basis and if any suspicious transactions are identified, the same shall be reported to FIU, Nepal.

Besides, in case of customer whose cumulative annual wire transfer is equal to or above NPR 5 crore in a fiscal year, the bank shall adopt following measures.

- The bank shall develop appropriate alert mechanism for cumulative wire transfer totaling NPR 5 crore or above.
- Accounts that fall under this category shall be treated as high risk accounts.
- Concerned branch offices shall conduct an annual assessment and document the same via ECDD internal observation form and same shall be report to central compliance.
- The compliance department shall monitor high value wire transfers on a quarterly basis and if any suspicious transactions are identified, the same shall be reported to FIU, Nepal.

Bank shall develop a SOP for processing high value wire transfer within a reasonable time frame to minimize the ML/TF risks inherent in such transactions.

If wire transfer with unclear purpose and/or inadequate document is found to be suspicious, in that case, it shall be the duty of bank to either reject or hold the transfer and report the same to the concerned authority.

3.10. Provisions relating Branchless Banking

The provisions relating to CDD and record retention also applies to the BLB customers. It shall be the duty of the concerned branch office to obtain necessary information and documentation, as per the provision of this chapter, prior to opening of accounts.

CHAPTER 4

BENEFICIAL OWNER

4.1. Introduction to Beneficial Owner

Beneficial owner is a natural person who ultimately owns or controls the account of other person. However, if a member of a family or the person who has power of attorney conducts the transaction, the same shall not fall within the purview of beneficial ownership. Beneficial ownership has a different connotation/implication in case of natural and legal person which has been explained below.

4.1.1. Beneficial owner in case of natural person

Beneficial Owner (BO) in case of natural account is a natural person/s other than the account holder who has ultimate control over the account. The beneficial owner uses other's account for his/her personal benefit which could range from tax evasion to any other predicate offence of money laundering.

Beneficial owner is different from beneficiary. A beneficiary/nominee is an individual or entity to whom a deceased benefactor known as a decedent bequeaths the balance of his/her account whereas beneficial owner is a person who ultimately controls the account. Branches shall conduct adequate due diligence to identify whether the beneficial owner and the legal owner is same or different person. Some of the indications where legal owner and beneficial owner are different person are mentioned below. Notable is the fact that the following instances are only illustrative in nature and are not exhaustive in nature.

- A Person opening account in name of his staff, driver, maid etc.
- A person opening account in name of his friend and depositing his money for structuring.
- Clue – e.g. Huge amount of deposits / unusual transaction in the account of a student/housewife/minor
- Clue –A person other than accountholder who frequently deposits and withdraws money from the account.
- Clue – e.g. Huge turnover from the accounts of person with low economic background.
- Potential sources for the identification of beneficial owner

4.1.2. Ultimate beneficial owner in case of legal account

Ultimate Beneficial Owner (UBO) is a natural person who exercises ultimate control over a legal person, entity or an arrangement. For instance, if the significant proportions of shares of company say 'ABC' is held by another company say 'XYZ' then it shall be pertinent to get the information of major shareholders of company 'XYZ' and this process shall continue till the

natural person who ultimately owns "ABC" is identified. Unlike in natural account, the legal shareholder could be the ultimate beneficial owner in case of a legal account but for that an in-depth analysis of ownership structure is required.

4.2. Importance of Beneficial Owner Identification

It shall be the responsibility of the bank to know its customers and their transaction. Identification of the beneficial owner and ultimate beneficial owner is a part of CDD process which helps the bank to identify its real customer and analyze the possible impact of their transactions. The rationale behind identifying beneficial owner is presented below.

- **Regulatory requirement** – NRB directive no 19 and FATF recommendations have provisions for the identification of beneficial owner.
- **To curb ML/TF activities** – Placement, which is the first stage of money laundering, is generally conducted using schemes like smurfing/structuring. The schemes like smurfing and structuring is usually effected by using accounts of other person which necessities requirement of identifying beneficial owners at the stage of account opening.
- **Risk profiling -** Accounts with different beneficial owner and legal account holder poses greater risk of money laundering as a result of which such accounts are categorized as high risk accounts.
- **Regulatory focus -** The focus of anti-money laundering guidelines is to identify person who has the ultimate level of control or entitlement. Thus, beneficial owner identification enhances better regulatory implementation.
- **Financial literacy**- It is believed that the focus of beneficial owner identification, on the part of bank, at the account opening stage, indirectly promotes financial literacy as a result of which innocent people can be protected from being victims of various money laundering schemes.

4.3. Beneficial Owner Information Collection and Analysis

It shall be the responsibility of the branches to collect beneficial owner and ultimate beneficial owner information from the customers during each of the following stages:

- During the process of establishing business relationship.
- During KYC update or enhanced customer due diligence.
- During each and every transactions conducted by high risk customers.
- During the time of change in ownership structure of a legal entity and
- During any suspicious activities conducted by the customer.

Branches shall consider the following sources while obtaining beneficial ownership information:

- Obtain the information from customer by self declaration,

- Obtain the information available publicly;
- Analyze the information available in social sites;
- Obtain the information maintained as per prevailing law,
- Obtain the statistics from business domain and
- Request the information from the concerned government entities.

4.4. Steps for Beneficial Owner Identification

Branches shall follow various steps while obtaining and processing beneficial ownership information which has been elaborated below:

Natural account

- Request the customer to self declare whether the account holder and beneficial owner are same person or not in account opening form,
- If answer is “Yes”, i.e. if the beneficial owner is different from that of account holder, ask the beneficial owner to fill up a separate KYC form,
- Categorize the customer under high risk category,
- Conduct enhanced customer due diligence,
- Additionally – Sources like social media, published information, other database etc should be used to identify beneficial owners (NRB directive -19).
- In case a person establishes business relationship or conducts transaction on behalf of another natural person, branches shall conduct customer due diligence of that person and obtain valid “power of attorney "so as to establish or rule out the presence of beneficial ownership in such cases.

Legal Account

- Analyze the ownership structure of the legal account.
- Identify the major shareholders of the holding legal entity, if it holds shares more than 10% of total shares of any other legal entity.
- Continue the process until the ultimate beneficial owner, i.e. the natural person who holds the major shares of the company is identified.
- Categorize the customer under high risk category.
- Conduct enhanced customer due diligence.

CHAPTER 5

POLITICALLY EXPOSED PERSON

5.1. Establishing Business Relationship with PEP

- Before establishing any relationship like account opening, occasional transactions or during KYC update, it shall be ensured whether or not the customer or beneficial owner is a PEPs, a family member of PEP ora close associate of PEP via screening and other means.

- The following sources shall be considered for collecting information related to PEP:

    - Obtain the information from customer (from declaration in account opening form and from interview),
    - Conduct screening through AML system used by the bank.
    - Obtain the information available publicly,
    - Analyze the information available in social sites,
    - Obtain the information maintained as per prevailing law and
    - Acquire PEP data from reliable source.

- In case the name of the customer or his/her family members or nominee of that person or beneficial owners matches under PEP list, the employee entrusted with the screening function should carry out adequate due diligence to ensure whether the match is accurate or not. The employee should verify whether the name, address and office information of the customer also matches with the list or not. If all these information are 100% matched, the concerned staff shall categorize the customer under high risk category and conduct enhanced due diligence.

- In case the customer or his/her family members or nominee of that person does not match under any PEP list but the staff has unconfirmed reason to believe that the person is PEP or associated with PEP, then in that case also the customer shall be considered as potential PEP and categorized under high risk category.

- Prior approval of senior management is mandatory before opening the account or before establishing any kind of relationship with PEPs and PEPs Associates.

- Enhanced due diligence shall be conducted for all the PEP customers which includes,*inter alia*, taking measures to establish source of funds and source of wealth.

- A customer shall be categorized as high risk customer if he/she is a family member or close associates of PEP.

- A customer shall be categorized as PEP even if the PEP status of such customer could not be confirmed or ruled out with substantial accuracy.

- Enhanced ongoing monitoring should be conducted for all the PEP customers.

- The provisions relating of PEP customer also applies to their family members and close associates.

5.2. PEPs Data and Update

- The Bank shall collect PEPs data at least once a year from the GoN or Government entities and prepare the PEPs list accordingly. Alternatively, the bank can also purchase PEP list from reputed vendors which shall include domestic, international and foreign PEPs.

- The purchased PEP data shall also include family members and close associates of PEPs.

- ThePEP data purchased should be updated on a periodic basis and any addition or removal of the same shall be brought into the notice of the Compliance Department accordingly.

- Batch screening of all the customers shall be conducted against PEP list on a quarterly basis.

CHAPTER 6

ONGOING DUE DILIGENCE

6.1. Introduction to Ongoing Due Diligence

Ongoing due diligence is a process of scrutinizing/monitoring transactions undertaken by its customers throughout the relationship to ensure that the transactions being conducted are consistent with the bank's knowledge of the customers, their risk profile and occupation or nature of business. The bank also ensures that the data, information and documents collected through customer due diligence process are kept up to date and relevant.

As a part of ongoing due diligence, the bank shall ensure the following:

- KYC information and documents of customers are up to date in the KYC/Account opening form, CBS and AML system.
- KYC information of high risk customers (including PEPs and beneficial owner) are updated every year and required documents are kept up to date.
- Transactions conducted by high risk customers are closely monitored.
- Cross border transactions are closely monitored.
- Threshold transactions are timely reported to FIU.
- Suspicious transactions if any are timely reported to FIU.
- Enhanced due diligence is conducted for high risk customers, if any identified or migrated post on boarding.

6.2. Transaction Monitoring

The Bank shall ensure a sound AML system in place to detect unusual/ suspicious activities/ transactions. Once the customer is on-boarded, monitoring the relationship, transaction, and activity of customer/s shall be done by the Bank. AML system of the bank shall be the primary tool to flag abnormal/suspicious transaction based on different rules set in the system like under threshold repetition , large cash transactions etc.

Inter alia following cases might require close monitoring of the transactions:

a) Transactions beyond KYC declaration,
b) Unusual activities/transactions/behavior,
c) Transaction without or unclear economical/legal objectives,
d) Large Cash transactions and
e) Other suspicious grounds as deem necessary by the bank.

Bank shall monitor use of its cards in foreign soil by its customers and assess whether or not the use of same matches with the information submitted by customer. Similarly, it shall also monitor the use of cards issued by foreign banks and financial institutions through its platform. While monitoring, if the transaction/activities are found to be suspicious, it shall be duty of the bank to withhold transactions from such card and report the same to FIU and other concerned authority.

6.3. Threshold Transaction Detection & Reporting

The Bank shall report threshold transactions as defined by regulatory body within 15 days from the date of transaction to the Financial Information Unit (FIU) as per format prescribed by the regulatory body. The AML System of the Bank shall generate such report on a daily basis.

6.3.1. Threshold Transaction Detection

Threshold transactions detection is the first step of reporting. Following are threshold transactions limit as defined by the Nepal Rastra Bank.

- Cash deposit or withdrawal equal to or more than Rs. 1 million in one transaction or in a series of transactions in one day in single account.
- Cross border electronic or other transfer equal to or more than Rs. 1 million by a customer in single or in a series of transactions in one day.
- Exchange of foreign currency equivalent to 5 lakhs or more by a customer in one transaction or in a series of transactions in one day.

6.3.2. Threshold Transaction Reporting

Threshold transactions shall be reported to FIU within 15 days via goAML application. It shall be the responsibility of branches to ensure that KYC of accounts crossing threshold limit is updated.

The Bank shall report TTR:

- If the cash deposit transaction equals or exceeds Rs. 1 million in one transaction or in a series of transactions in one day in a single account.
- If the cash withdrawal transaction equals or exceeds Rs. 1 million in one transaction or in a series of transactions in one day in a single account.
- If the total of cash debit or credit transaction mentioned in i) and ii) exceeds Rs. 1 million individually i.e either deposit total or withdrawal total.
- TTR reporting should be separate for each of above mentioned category of TTR i.e.. TTR-Cash, TTR-Cross Border and TTR-FCY exchange in goAML. The TTR guidelines issued by FIU should be taken into consideration while categorizing the threshold transactions.

- If the threshold reporting limit in either side of any category of TTR equals or exceeds then entire transactions related to that category should be reported.

Note:

- The threshold amount may be reached by a single transaction or by a series of transactions in cash\transfer into a single account or by a single customer over a period of one working day. It may be considered to be an aggregate transaction in cash\transfer exceeding the prescribed threshold within a single day.
- Cash does not include negotiable instrument, nor does it include a transfer of funds by means of bank cheque, bank draft, electronic funds transfer, wire transfer or other written order that does not involve the physical transfer of cash. These methods of transferring funds do not fall within threshold reporting obligation.
- Customer shall be required to mention source of fund and purpose of transaction in every cash deposit from NRs. 1,000,000 or above in a single or several transactions in a day. However, source of fund and purpose of transaction shall be required for all the amounts in case threshold transaction limit is exceeded in a day.
- Customers shall declare that the fund is not earned from any illegal activities including Terrorism, drugs dealing, human trafficking and/or any organized crime (The customer has to present supporting documents if required).
- With respect to foreign currency transactions, the threshold amount stated above shall mean the amount derived by multiplying the same at the prevailing exchange rate on that date.

Steps for goAML Reporting

- Transactions that cross threshold limit as mentioned above is triggered by the AML system.
- goAML reporting team shall check the transaction, KYC information and other details required for reporting.
- Such transactions shall be reported within 15 days via goAML.
- Branch offices shall be responsible for any non reporting of threshold transaction if the same is due to non update of KYC in the core banking system of the bank.
- Head of Compliance department shall be updated on daily basis.

6.3.3. Exempted transaction to TTR reporting

The Bank shall not submit the threshold transaction detail of the followings to the FIU.

- Transaction conducted by Government of Nepal, its offices and entities,
- Transactions conducted by entities established under special acts,

- Transactions conducted byBFIs with itself or with other licensed BFIs or with government entities,
- Transaction of Government or semi government offices, Association, Institution, Company or Entities and entities established under special Act,
- Reinsurance transactions of insurance companies,
- Transactions related with loan disbursed by BFIs to its customers according to prevailing laws.
- Transactions related with staff facilities provided by BFIs to its employees,
- Transaction conducted by UN, offices under UN and other International organizations,
- Fund transfer (except cash) from the account of one BFIs to the account of other BFIs via cheque within Nepal.
- Amount deposited by customers as fees in the account of School, College, Universities or Hospitals.
- Amount deposited by insured in the account of insurance company as insurance fee.
- Transaction related with pension payments of Nepal Police, Nepal Army and other institutions.
- Transactions conducted in the internal accounts of BFIs like settlement accounts, Nostro/Vostro accounts etc.
- Institutional transactions conducted by cooperatives and national cooperative bank ltd.
- Transactions occurred while opening LC or making payment related to LC transactions.
- Other transactions exempted for reporting as per NRB Directive from time to time.

Note: Threshold transactions shall change based on changes in FIU requirements from time to time.

6.4. Suspicious Transaction Generation Analysis and Reporting

Transactions conducted by the customer become suspicious when they deviate from the customer profile orKYC information provided to the Bank. Further, transactions that exhibit the indicators of illegality shall also be categorized as suspicious transaction. Suspicious transactions shall be monitored and analyzed thoroughly and shall be reported to FIU after being confirmed.

Suspicious transaction reporting follows a process where the triggers are identified based on various rules. Identified/flagged transactions are then analyzed or examined using different tools and techniques. After being confirmed, such transactions are reported to FIU confidentially.

6.4.1. Generation of Suspicious Transactions

Generating suspicious transaction trigger is a crucial phase in transaction monitoring process.Following are the main sources from where suspicious transactions are generated.

1. **AML system**: The AML system shall generate/flag suspicious transactions on the basis of actual transactions conducted by the customer under different rules set. Some of the rules are under threshold repetition, large cash transaction, KYC deviation, and occupation deviations etc.

2. **Branch:** Customers visit branch to conduct transactions where they come into the direct contact with the branch staff. Branch staff can spot suspicious transactions, behavior or activities of their customer directly. So, branch is the second main source for the identification of suspicious transactions. Branch management shall communicate potential STR by filling up a STR form and reporting the same to the compliance department.

3. **Investigation Authorities:** If the information or report asked by investigation authorities during investigation includes subject related to suspicious transaction/activities of customers, such transaction/activities of customers shall be reported to FIU as STR/SAR.

6.4.2. Identification of Suspicious Transaction

If the generated suspicious transactions match any features or have any indicators mentioned below, then the transactions are identified as suspicious transactions.

6.4.2.1. Features of Suspicious Transactions

- Transactions having unclear economical and business target – E.g. frequent large cash deposit from different branches from different person in the account of a customer who owns a small tea shop.

- Transactions conducted in relatively large amount cash and/or conducted repeatedly and unnaturally – E.g. Deposit of 9 lakhs for 30 days in a month.

- Transactions conducted differently from that of usually and normally conducted by the relevant customer – E.g. Turnover of 50 crores in students account.

- Huge, complex and unusual transaction – E.g. sale of land to buy house and sale of house to buy car and sale of car to buy land etc. (Layering), FDI from Mauritius.

6.4.2.2. STR Triggers

General Indicators

I. Cash

- Transactions conducted in a relatively small amount but with high frequency (structuring).

- Transactions conducted by using several different individual names for the interest of a particular person (smurfing).
- If customer conducts series of transactions or bookkeeping tricks for concealing the source of fund (layering).
- If customer consistently makes cash transactions that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.
- The purchase of several insurance products in cash in a short period of time or at the same time with premium payment entirely in a large amount and followed by policy surrender prior to due date.
- If person sending money cannot provide even general information about the recipient of money.
- If anyone attempts to transfer or receive amount in a suspicious manner.

II. Economically irrational transactions

- Transactions having no conformity with the initial purpose of account opening.
- Transactions having no relationship with the business of the relevant customer.
- Transaction amount and frequency are different from that of normally conducted by the customer.

III. Behavior of the Customer

- Unreasonable behaviors of the relevant customer when conducting a transaction (nervous, rushed, unconfident, etc.)
- Customer with significant Money Laundering, Terrorist Financing and Proliferation Financing related adverse news or other indicators relating to financial crime.
- If customer shows unusual curiosity about internal system, control and reporting.
- If customer admits or makes statements about involvement in criminal activities.
- If customer offers money, gratuities or unusual favors for the provision of services that appear unusual or suspicious.
- If customer/prospective customer gives doubtful or false information with respect to his/her identity, sources of income or businesses.
- If customer/prospective customer uses identification document that is unreliable and refuses to provide information/documents requested by the officials of the relevant reporting entity without any valid reasons.
- If customer or his/her legal representative tries to persuade the officials of the relevant reporting entity not to report his/her transaction as a Suspicious Financial Transaction.
- If customer opens the account for a short period and closes without a valid reason.
- If customer is unwilling to provide right information or immediately terminating business relationship or closing his/her account at the time the officials of the relevant reporting entity request information with respect to his/her transaction.

- Only online transactions are done in the customer's account, in such case there can be separate beneficial owners.

IV. Employees and Agents of REs

- Changes in employee characteristics, (e.g. lavish lifestyles or avoiding taking holidays).
- Changes in employee or agent performance.
- Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

V. Use of third party

- Multiple deposits made to an account by non-account holders.
- Unrelated parties sending fund transfers or other forms of electronic transfers to the same beneficiary with no apparent relation to the recipient.
- If a client conducts transaction while accompanied, overseen or directed by another party.
- If a client makes numerous outgoing payments to unrelated parties shortly after they receive incoming funds.
- Wire transfers, deposits or payments to or from unrelated parties (foreign or domestic).
- If a client appears or states to be acting on behalf of another party.
- Account is linked to seemingly unconnected parties.
- If power to attorney to operate account is given to third party.

VI. Corporate and Business Transactions

- If accounts are being used to receive or disburse large amounts but shows no normal business related activities, such as the payment of payrolls, invoices, etc.
- If the transaction is not economically justified considering the account holder's business or profession.
- If business transactions is found to be done through personal accounts.
- If customer makes a large volume of cash deposits from a business that is not normally cash-intensive.
- If customer does not want to provide complete customer due diligence information of their business.
- If the financial statements of the business differ noticeably from those of similar businesses without valid reasons.
- If size of wire/fund transfers is inconsistent with normal business practice/transactions for the customer.
- If unexplained transactions are repeated between personal and business accounts.
- If deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations (e.g. Cheques, Letters of Credit, Bills of Exchange, etc.)

VII. Wire/Funds Transfer Activities

- If customer fails to provide adequate information about the originator, beneficiary, and purpose of the wire transfer.
- If customer orders wire transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- If the pattern of wire transfers shows unusual patterns or has no apparent purpose.
- If customer receives frequent fund transfers from individuals or entities who have no account relationship with the person/institution.
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
- If several customers request transfers either on the same day or over a period of two to three days to the same recipient.
- If beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activities.
- If customer conducts series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
- Fund transfers to and from high-risk offshore financial centers without any clear business purpose.
- Fund transferred to and from high risk jurisdictions and sanctioned countries.
- Receipts of fund transfer in several phases and once accumulated the funds are subsequently transferred entirely to other account.
- Receipts/payments of funds made by using more than one account, either in the same name or different names.
- Fund transfers using the account of reporting entities' employee in an unusual amount.
- Remittance and donations are received on personal account whereby the use of the fund is not clear e.g. fund received for day to day transactions of school, monastery, church, Madarsa etc.
- If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.

VIII. Lending

- If customer makes a large, unexpected loan payment with unknown source of funds, or a source of fund that does not match what the credit institution knows about the customer.
- If customer suddenly repays a problematic loan unexpectedly without a valid reason.
- If customer repays a long term loan, such as a mortgage, within a relatively short time period.
- If the source of down payment is inconsistent with borrower’s financial ability, profession and business as per the declaration.
- If customer shows income from foreign sources on loan application without providing further details.

- If customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.
- If the loan transaction does not make economic sense (e.g. the customer has significant assets, and there does not appear to be a valid business reason for the transaction).

IX. Trade Based Money Laundering

- Submitting the fake documents and false reporting by the customer such as commodity misclassification, commodity over- or under-valuation etc.
- If the transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification.
- Phantom shipping – If no goods are shipped and all documentation is completely falsified to move funds in the guise of trade.
- Payments to the vendor by unrelated third party.
- If the customer trades commodities that do not match the nature of business of the customer.
- If the commodity is shipped to (or from) a jurisdiction designated as "high risk" for money laundering activities.
- In case of Double-invoicing.
- If there are significant discrepancies between the descriptions of the goods on the transport documents, the invoice, or other related documents.
- If customer is involved in potentially high-risk activities, including those subject to export/import restricted goods such as weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials etc.

X. Other Indicators

- If transaction seems to be inconsistent with the customer's apparent financial ability or profession or usual pattern of financial transaction as per the declaration.
- If customer attempt to open or operate accounts under a false name.
- If transaction involves a country known for highly secretive banking and corporate law.
- If customer shows reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify.
- Opening accounts when the customer's address or employment addresses are outside the local service area without a reasonable explanation.
- There is a sudden change in customer's financial profile, pattern of activity or transactions.
- Customer uses notes, monetary instruments, or products and/or services that are unusual for such a customer.
- If unknown third party frequently transfer funds into customer's account.

- If there is suspicion on the transaction of the customer who is blacklisted by Credit Information Bureau or the reporting institution itself has placed the concerned customer in a high-risk customer category.
- If customer is suspected for using of personal account for business or other purposes, or vice-versa.
- If customer fails to provide reasonable justification for the transaction.
- If customer conducts series of complicated transfers of funds that seems to be an attempt to hide the source and intended use of the funds.
- If unnaturally huge amount is transferred to the name or account of any foreign citizen, tourist, student, visitor, worker or a person recently migrated to Nepal from the country or region where terrorist organizations operate.
- If unrelated third party is unnaturally, unnecessarily involved or is more active in transaction.
- If multiple personal and business accounts are being used to collect and then channel funds to foreign beneficiaries of the countries known or suspected to facilitate money laundering activities or terrorism financing.
- If there is repeated transfer of money to and from the name of foreign individual or the individual living outside Nepal without any valid reason.
- If customer has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- In case of large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- If account has close connections with other business accounts without any apparent reason for the connection.
- If deposits to or withdrawals from a corporate account are primarily in cash.
- If customer requests movement of funds that are uneconomical without any valid justification.
- If customer visits the locker (safety deposit box) area immediately before making cash deposits.
- If customer repeatedly conducts large foreign exchange transactions.
- If any suspicious pattern emerges from customer's transactions.
- If customer is found to have used/made or involved with counterfeit coin and currency.

6.4.3. Suspicious transactions analysis/examination

Identified suspicious transactions need thorough examination or analysis for being confirmed that they are suspicious transactions. Analysis of account statement, KYC information and branch view helps to identify and confirm the suspicious transactions. After completion of this stage, it shall be decided whether or not to report the transaction trigger as STR. However,

6.4.4. Suspicious Transaction Reporting

Suspicious transactions shall be reported to FIU once they are identified and confirmed. The compliance department shall report suspicious transactions as soon as possible within three days of being confirmed that they are suspicious transactions. Such reporting shall be done via goAML application.

6.4.4.1. Steps for suspicious transaction reporting by branch office to central compliance:

- Assess transactional and behavioral pattern of customers by way of monitoring and observation.
- Examine unusual activity with the following elements.
    - Transaction deviating from the profile; the characteristics; or the usual transaction pattern of the relevant customer.
    - Transaction reasonably suspected to have been conducted with the purpose of evading the reporting that must be conducted by the relevant reporting entity.
    - Financial transaction conducted using fund alleged to be attributable to predicate offences.
    - Transaction that have no economic or legal rationale or bonafide purpose.
- Examine the KYC information of the customer, account statement, and other documents obtained during account opening.
- Gain additional information about the customer from the branch office, any other person or any other source as may seem reasonable.
- Evaluate all above information obtained regarding customer.
- If the transaction seems suspicious or unsure, prepare a Suspicious Transaction Report in the format prescribed by FIU and send to the Compliance Department.
- Ensure that the customer is not informed about the enquiry and investigation by any means.
- Suspicious transaction reporting should be kept highly confidential.

6.4.4.2. Steps for suspicious transaction reporting by Central Compliance to FIU:

- Analyze the suspicious transaction reports sent by the branch along with the account opening form, KYC form, account statement and other documents.

- Analyze the red alerts generated in the AML system along with the account opening form, KYC form, account statement and other documents.

- If seems suspicious, prepare a STR form as prescribed by FIU and send necessary documents/information to FIU via goAML as soon as possible within 3 days.

- Suspicious transaction/activities of PEPs shall be categorized as STR-PEP, Suspicious transaction/activities related to trade based money laundering shall be categorized as STR-TBML and other suspicious transaction/activities shall be categorized as STR-High, STR-Medium, STR-Low according to the internal policy/procedures.

- The bank shall consider "STR/SAR Guidelines", "goAML Operational Guidelines" or other guidelines while preparing STR/SAR.

- The bank shall stop the KYC update process and send STR/SAR to FIU in case it is sensed that KYC update process could tip off the information related to suspicious transaction/activity reporting to customer.

6.5. Suspicious Activity Reporting (SAR)

Bank shall report suspicious activities of its customers, including attempted suspicious transactions, to financial information unit. The suspicion shall be based on the risk of money laundering and/or terrorism financing. It shall be responsibility of the branch offices to monitor activities of the customers and report all money laundering and terrorism financing prone suspicious activities of its customers to the Compliance Department. The Compliance Department shall conduct necessary investigation on the activity and report the activities if it deems necessary.

It shall not be mandatory for the compliance department to report all the SAR received by it from the branch offices.

6.6. Standard Operating Procedure

It is understood that standard operating procedure brings uniformity in suspicious transaction related analysis and reporting. The bank shall develop standard operating procedure in relation to suspicious transaction and suspicious activities reporting process with an objective to enhance the degree of efficiency and effectiveness.

6.7. Confidentiality of the Information

The bank, its directors, officers and employees shall not disclose to its customer or to any other person that a particular report, document, record, notice or information concerning suspected money laundering or terrorist financing or predicate offence has been initiated or is being submitted to FIU and/or any other enforcement authorities and their officers. The lists of such non-disclosable cases are as follows.

- Report of suspicious or threshold transaction.
- Report of suspicious activities.

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

The bank shall take departmental action if any designated person or staff tips off the confidential information/record/notice/report to its customer or other person.

6.8. KYC Information Update

KYC information of all the customers shall be updated on a continuous basis. The Bank shall apply risk based approach to update the information of its customers in the core banking system as well as in terms of documentation.KYC information of the customers shall be updated on the basis of following:

6.8.1. Periodic Basis

- High risk customers: To be updated at least once a year.
- Medium risk customers: To be updated at least once in 3 year.
- Low risk customers: To be updated at least once in 5 years.

The Bank shall develop a system to ensure that KYC information of high risk customers are updated annually and required CDD measures are applied accordingly.
Irrespective of risk categories, in some situation the customer information need to be updated immediately. The Bank shall ensure that in following cases KYC information of the customer is updated immediately.

Bank shall maintain a separate list of "KYC not updated customers/account holders"which cannot be updated even after exercising best effort on the part of bank.

6.8.2. Trigger basis

The bank shall ensure that KYC of customers is updated on an immediate basis in case following trigger events are materialized:

- CDD process is not complete,
- KYC information is not complete or missing in the Account Opening/KYC form,
- Transactions/behavior of the customers seems suspicious,
- Changes in customer's information like occupation, annual income, and annual turnover, present address etc.
- Doubt about veracity or accuracy of the previously obtained customer identification data.

The Bank shall ensure that following points are taken into consideration during KYC update process.

- Where there are changes in KYC information of the customer or where KYC information is incomplete obtaining only changed/missing information shall be sufficient and entire KYC information need not be obtained.
- Self-presence of the customer shall be mandatory for the KYC information like name, permanent address, citizenship, photograph and signature etc. which are permanent in nature, whereas for other information like occupation, nature of business, income, turnover etc. which can vary time to time, customer presence shall not be mandatory. Such information can be obtained from telephone, email or other means. However, the bank should ensure its reliability and validity.
- The bank shall develop a separate list of unreachable customers who do not come to the contact of the bank for the purpose of KYC update even after the best effort.
- KYC update shall mean update in CBS and AML system as well.
- Provisions relating to periodic and trigger based KYC update shall apply to information contained in both the AML system and core banking system of the bank.

6.9. KYC Documents update

The branch shall ensure that incase of legal accounts, updated documents are obtained while updating the KYC information. It includes

- Updated financial statements
- Updated AOA, MOA, Board minute, power of attorneyetc
- Other documents if any.

6.10. Remote Updates

Remote update refers to the process of updating customer information in the CBS and or AML without customer being physically present at the bank premises. Remotes updates can be done by obtaining information through telephone or mail or some other electronic format. However, bank shall ensure the reliability and documentation of information so obtained. Remote updates shall be done only in case of information which are changeable in nature (for example temporary address, mobile no., occupation/business, income, turnover, PEP/FATCA/BO declaration, nominee information etc) and shall not be allowed in case of information which are considered as permanent in nature. The following provisions shall be noted regarding remote updates:

a) Remote update can be done by KYC call center of the bank or by the branch staff authorized by branch manager in this regard.
b) Remote update shall be done only in case of information which are variable in nature.
c) When information is obtained through mail, bank shall maintain adequate documentation thereof.

d) Information Technology Department of the Bank shall gradually devise a mechanism to record and retain audio clips, files of conversation when Remote update is done on the basis of telephonic conversation.

e) Bank staff shall behave in a polite manner and maintain professional courtesy while obtaining information from customer for the purpose of Remote update.

6.11. KYC Update Form

KYC of all the High risk, Medium risk and Low risk customers shall be updated after every one year, three years and five years respectively. However, filling up of complete account opening form on every KYC update cycle leads to duplication and redundancy. Thus, a separate KYC update form will be developed to capture only such data of customer that varies over time.

6.12. Other Provisions

Bank shall obtain complete documents at the time of opening of accounts and in addition audited financial statement of previous financial year should be obtained in case of entity. However, documents to be obtained at the time of subsequent KYC update shall bedeterminedon the basis of risk.

CHAPTER 7

ROLES AND RESPONSIBILITIES

7.1. Roles and Responsibilities of AML/CFT Board Level Committee

AML/CFTBoard Level Committee shall constantly oversight the function related to AML/CFT of the Bank. The roles and responsibilities of AML/CFTBoard Level Committee related to this policy are as follows:

- To submit the report of activities performed under AML/CFT Act, Rules and NRB Directives to the Board of Directors.
- To discuss the adequacy of Policy and Procedures formulated under AML/CFT Act, Rules, NRB Directives and FATF recommendations.
- To suggest the BOD regarding the measures applied for the identification and control and money laundering and terrorism financing and adequacy of information system used for AML/CFT.
- To formulate and effectively implement customer identification and acceptance policy that incorporates risk based approach, PEPs and beneficial owner.
- To submit a quarterly report to BOD regarding compliance and implementation status of AML/CFT Act, Rules and NRB Directives and internal policy of the Bank.
- To obtain following reports from the management and suggest the BOD as required
    - AML/CFT risk management report,
    - Report including KYC update status, details of CDD, details of PEPs, details of ECDD,
    - Report including discussion/suggestion over the comments/remarks mentioned in internal and external auditing report and internal monitoring report of the Bank regarding money laundering and terrorism financing.
    - Report including the detail analysis of ML/TF risk inherent while launching new product/services, purchasing IT system, conducting wire transfers, conducting fund transfers through electronic banking and suggestions for improvement in policy and procedures.
- To review ML/TF risk assessment related to new products and services, purchase of IT system, wire transfers and transactions related to E-banking, mobile banking (including QR), mobile wallet, and online services offered by the bank and suggest for policy and process level changes, if required.
- To analyze the possible impact of money laundering and terrorism financing activities/events happening in both national and international level and submit suggestion to BOD for its management.

- To organize training and knowledge sharing program for compliance officer, shareholders holding more than 2% of paid up capital, members of BOD, top management and employees directly involved in AML/CFT day to day activities.
- To ensure that the bank is submitting reports asked in directive no. 19 via mentioned channel maintaining confidentiality in a regular basis.
- To perform the roles and responsibilities delegated by the Board of Directors.
- To monitor and oversight the implementation status of AML/CFT Policy and Procedures.

7.2. Roles and Responsibilities of Compliance Department

- To conduct necessary monitoring so as to ensure that proper due diligence is done before on boarding of customers.
- To review the existing policy and assess the policy GAP in the areas relating to compliance function of RBBL.
- To conduct annual AML/CFT risk assessment of the bank.
- To take necessary steps to ensure that proper due diligence is done in case of all the account holders.
- To monitor compliance with requirements of correspondent banks to the extent compliance is related to AML/CFT.
- Operate and supervise KYC call center of the bank.
- goAML reporting of TTR and STR.
- To monitor transactions through AML system of the bank and conduct necessary reporting if required.
- To reply to the external agencies (CIB, FIU, Nepal police etc.) queries.

7.3. Roles and Responsibilities of Compliance Officer

- To get access to any record, statement, books or accounts required to perform the activities.
- To ask/obtain documents/record/statements/information from the employees of the bank.
- To perform required activities to implement the AML/CFT act, rules and directives.
- To perform other regulatory requirements.
- To act as a focal point for the effective compliance of prevailing acts, rules and directives related to AML/CFT.
- To formulate and submit the draft of policy/procedures/system in order to effectively comply act/rules/directives.
- To analyze/check the unnatural/suspicious transactions obtained from departments designated officials and employees.
- To get the documents/statements/information from other departments and designated officers at any time without any hassles in order to perform the activities.

- To monitor the compliance status of prevailing acts/rules/directives/guidelines and submit the report.
- To recommend for departmental action on employees/office bearers of the bank who do not provide adequate information and documents during the course of complying with the provisions of various acts, rules and regulations. Further, it shall be the duty of bank to act upon such recommendation for departmental action done by compliance officer. Information on such departmental action shall be provided to FIU on a timely basis.

7.4. Roles and Responsibilities of Head of Compliance

- To facilitate effective compliance with prevailing acts, rules and directives related to AML/CFT in compliance department.
- To formulate annual action plan of compliance department.
- To conduct overall AML/CFT risk assessment of the bank on an annual basis.
- To review the policy and procedures on a need/periodic basis.
- To arrange/participate the meeting with management level and board level AML/CFT Committee periodically.
- To give necessary directions/ guidelines/approvals to Compliance Department.
- To analyze/review the suspicious reports submitted by the employees/branches

7.5. Roles and Responsibilities of IT Department

- To provide all IT related services and data for the implementation of AML/CFT Policy and Procedures.
- To own the process followed for obtaining data for the purposes of regulatory reporting.
- To review the mechanism followed for searching accounts centrally and ensure that the same is accurate.
- To act as a liaison between core banking system and AML system.
- To perform all IT related activities for the effective implementation of AML system.
- To streamline all the IT related procedural aspects for goAML reporting.
- To update the fields in core banking system as per the requirement.
- To provide reports as required by compliance department.
- To provide all necessary data for regulatory reporting within prescribed timeline.
- To ensure accuracy of data provided to compliance department for regulatory reporting.
- To review the existing AML system of the bank on a periodic basis in coordination with Compliance Department.

7.6. Roles and Responsibilities of Internal Audit Department

Role and Responsibilities of Internal Audit Department has been specified below.

- Internal Audit Department shall assess the effectiveness of AML/CFT Policy.
- Internal Audit shall assess compliance status of the AML/CFT Policy and Procedures of the bank independently.
- Internal Audit Department shall assess the risk inherent in AML/CFT function of the bank and assess the controls.
- The Internal Audit Department shall include "review over AML/CFT function" as part of their scope while conducting branch audit.
- The Internal Audit Department shall include follow up of NRB observations on AML/CFT function of the Bank as part of their scope while conducting branch audit.

7.7. Roles and Responsibilities of Branch Operation Department

The branches and the BOD of the bank shall act as a first line of defense to ensure that AML/CFt related policy and procedures are complied with. The compliance department shall act as a second line of defense in this matter. In light of this principle relating to allocation of responsibilities, the following key responsibilities of BOD has been mentioned below.

- To act as a liaison between branches and Compliance Department.
- To address branch related problems related to Customer Due Diligence
- To review and update the compliance and AML/CFT matter in branch operation manual in line with the changes in regulatory requirement and prevailing laws.
- To ensure that compliance with AML/CFT in branch level is not affected due to shortage of forms and other logistics support.
- To take ownership over CDD function as a part of branch operation and ensure the KYC of all the accounts are updated over time.

7.8. Roles and Responsibilities of Legal Department

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

7.9. Roles and Responsibilities of Human Resource Department

Human Resource Department is responsible for smooth supply of human resources in Compliance Department. The roles and responsibilities of Human Resource Department related to this Policy shall be as follows:

- To ensure smooth supply human resources in compliance department
- To ensure that employee due diligence and background verification is conducted before appointing any employee.
- To ensure that employee due diligence is conducted periodically andappropriate record is maintained appropriately.
- To provide training to human resources in the area of AML / CFT on need basis.

7.10. Roles and Responsibilities of Senior Management

Senior management of the bank comprises of Chief Executive Officer, Deputy Chief Executive Officer and Assistant Executive Officer. The main function of senior management in relation to this policy is to get the policy and procedures implemented in an effective and efficient way. The roles and responsibilities of senior management have been mentioned below.

- To implement or cause to implement the policy and procedures.
- To monitor the activities of compliance department as per the compliance annual plan.
- To ensure that the bank has all the required procedural guideline in place to effectively achieve the objectives of this policy.
- To ensure cross departmental coordination so as to ensure that the compliance with AML/CFT Act/ Rules, Policy and Procedures due to matters beyond the control of compliance department.

7.11. Roles and Responsibilities of Provincial Offices

- To implement or cause to implement the policy and procedures in branches.
- To address the AML/CFT related problems of branches and communicate to top management accordingly.

7.12. Roles and Responsibilities of Branch Manager

- To ensure that branch staffs conduct customer due diligence procedures effectively and efficiently.
- To forward the report of unusual and suspicious transaction to Compliance Department.
- To implement or cause to implement the AML/CFT measures effectively and efficiently in branches.
- To respond to compliance notice issued by central office compliance department on a prompt basis.

7.13. Roles and Responsibilities of Employee

- To carry out Know Your Customer/Customer due Diligence procedures effectively and efficiently during customers on boarding.
- To update the information of customers in core banking system and AML/CFT system as required.
- To conduct preliminary risk profiling of the customers before opening the account.
- To continuously monitor the transactions of high risk customers.
- To report suspicious transactions/behaviors of customers to compliance department.
- To inform/educate/aware the customers about the beneficial owner.
- To provide the information/documents asked by compliance Department in stipulated time.
- To prepare and provide reports to Compliance Department in stipulated time and as per the requirement.
- To implement the AML/CFT measures effectively and efficiently.

CHAPTER 8

TRAINING AND AWARENESS

8.1. Employee Training and Awareness Program

Employee training program shall be the part of annual AML CFT program. The bank shall ensure following provisions.

- AML/CFT training shall be provided to all employees of the bank.
- Training should be provided on a periodic basis that shall include updates in AML/CFT regime, adverse media news related to ML/TF, regulatory requirements etc.
- Practical aspects like case studies and presentation; experience sharing, problem solving shall be the integral part of AML/CFT training.
- The underlying theme of AML/CFT training shall be "Business with Compliance".
- Special focus shall be provided to employee working in customer service desk, cash counter, credit and trade finance.
- Pre-service training
- Employees working in compliance department shall be given exposure to National and International training related to AML/CFT.

8.2. Knowledge Sharing Program

Knowledge sharing program related to AML/CFT shall be conducted for shareholders (holding more than 2% or more share of paid up capital), members of board of directors, top management and employees involved in day to day AML/CFT activities.

8.3. Online Training Portal

A training portal shall be developed and linked with the intranet from where employees can get knowledge related to AML/CFT, CDD and risk management. Training materials shall be timely added and updated.

8.4. Training Effectiveness

Training effectiveness refers to the quality of the training provided and measuring whether the training met its goals and objectives. Following questions shall be addressed while measuring training effectiveness.

- How did the participants react or respond to the training?
- What did participants learn from the training?
- Did the trainees take what they learned and put it into practice on-the-job?
- What is the impact of training on bank's profitability and sustainability?

CHAPTER 9

WALK-IN CUSTOMERS

9.1. Definition of walk-in customers

Walk-in Customer means a person who does not have an account based relationship with the Bank, but undertakes transactions with the Bank. The bank provides various services like remittance, foreign exchange etc. to walk in customers. From money laundering and terrorism financing perspective, walk-in customers pose higher risk to the bank due to following reasons:

- Since the walk-in customer does not have an account with the bank, it is very difficult to obtain full KYC information of the customer. Due to this reason, the bank cannot study the profile of the customer.
- The bank cannot monitor/track the transaction of the customers. For e.g. in case of remittance transaction, the same customer can withdraw cash more than one lakh from different branches of the bank using different remittance channel like RBB remit, city express, prabhu pay, ime, lalit money transfer etc. without having an account with the bank.
- There is high chance of customer being used by some otherbeneficialowner.For e.g. the beneficial owner can use passport/visa of other person to exchange the illegal foreign currency that s/he has which introduces high risk of money laundering to the bank
- In case of remittance transaction, there is high chance of money to be used in terrorism financingasthe sender can send money in small amounts to different beneficiaries.

9.2. Risk based Customer Due Diligence

9.2.1. Customer Screening

Customer screening is a process of screening the name and other details of customers against sanction and other lists to ensure that the sanctioned entity and individual is not involved in the transaction. At the same time, screening also helps in proper profiling of customers in terms of risk. If the name and other details match with the details of sanctioned individual/entity and black list, the concerned branch staff shall inform the compliance department and reject the transaction under the guidance of compliance officer. If the name matches under PEP/adverse media/investigation/black list or other list and the same is confirmed, the concerned branch staff shall categorize the customer under high risk category and conduct the transaction.

9.2.2. Customer Acceptance and Rejection

The walk-in customers pose high risk of ML/TF to the bank. The bank shall accept the customers after conducting necessary due diligence. The NRB directives and other prevailing laws prohibit the bank to establish the relationship with certain categories of customers. The bank shall reject to conduct the transaction in following cases:

- In case the bank cannot apply required CDD measures to conduct the transaction. For e.g. the customer cannot provide required documents like citizenship/other identity documents.
- In case the identity documents presented are false/fraud.
- In case the name of the customer matches with the sanction list or black list and the same is confirmed after following prescribed procedures as per para 9.2.1.

9.2.3. Customer Identification and Verification

The bank shall obtain and verify the following information/document of conductor/beneficial owner while conducting transaction with walk-in customers.

In case of remittance transaction in cash

- Full name of sender and beneficiary,
- Address of sender,
- Permanent and temporary address of beneficiary,
- Contact number of beneficiary,
- Relationship between the sender and the beneficiary,
- Source of fund,
- Purpose of transaction,
- Citizenship no. of conductor with issued district and issued date of customer/beneficial owner,
- If the beneficial owner of the transaction is other than the conductor of transaction then all the information of beneficial owner shall be obtained as mentioned above.

Note: The customer shall fillup separate KYC form for remittance transaction in cash.

In case of foreign exchange transaction in cash

- Full name/permanent and temporary address of customer,
- Father's and grandfather's name of customer,
- Passport no with issue and expiry date, issued authority and issued country,
- Valid visa,
- Plane ticket,
- Purpose of transaction and source of fund,

- If the beneficial owner of the transaction is other than the conductor of transaction then all the information of beneficial owner shall be obtained as mentioned above.

Note: The customer shall fill up separate KYC form for forex transaction in cash.

9.2.4. Risk profiling

The risk profiling for walk-in customer shall be based on following two criteria.

- KYC Profile based risk profiling:

Risk profiling based on the KYC profile of the customer shall be done before approving the transaction. The concerned branch staff shall categorize the customer under high risk category in case of following scenarios:

  - If the name of the customer matches with PEP/Adverse media/Investigation list,
  - If the customer shows unusual/suspicious behavior/activities.

- Transaction based risk profiling

Risk profiling based on the transaction of the customer shall be done after the completion of the transaction. The AML system of the bank shall be responsible to flag suspicious/unusual transaction of the customers as high risk transaction. The transaction based risk profiling of walk-in customers shall be done on following broad criteria

Ongoing Due Diligence

The bank shall conduct risk based due diligence for walk-in customer on an ongoing basis. Extensive monitoring /enhanced due diligence shall be done for the transactions conducted by high risk customers.AML system of the bank shall flag abnormal/suspicious transaction based on different rules set in the system like unusual transactions/activities/behavior of the customer. The bank shall categorize such transaction as high risk transaction and such transaction shall be monitored and reported if any suspicion is found.

9.3. Reporting Requirements

9.3.1. Reporting of suspicious transaction

The bank shall report suspicious transactions/activities of the walk-in customers to FIU, Nepal within three days after being confirmed that the transaction is suspicious. Some features of suspicious transactions are mentioned below:

Remittance transaction:

- If customer fails to provide adequate information about the originator, beneficiary, source and purpose of the remittance.

- If the same customer withdraws cash from different branches of the bank using different remittance channel exceeding one lakh in total in a day.
- If the beneficial owner of the remittance is other than the conductor.
- If customer frequently receives remittance in small amounts in an apparent effort to avoid reporting requirements.
- If the pattern of remittance shows unusual purpose/patterns or has no apparent purpose.
- If unrelated parties send remittance to the same beneficiary with no apparent relation to the recipient.
- If remittanceis received from high-risk offshore financial centers without any clear business purpose.
- If remittance and donations are received on personal account whereby the use of the fund is not clear e.g. fund received for day to day transactions of school, monastery, church, Madarsa etc.
- If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.

Foreign Exchange Transaction:

- If customer fails to provide adequate information about the source and purpose of the foreign currency exchange.
- If it is suspected that the foreign currencies are obtained from illegal sources.
- If the customer comes to exchange high value foreign currencies.
- If the beneficial owner of the transaction is other than the conductor.

9.3.2. Reporting of threshold transaction

If the foreign exchange transaction of the customer exceeds the threshold limit as mentioned in the NRB Directives, the bank shall report such threshold transaction to FIU Nepal within 15 days of the transaction.

9.3.3. Other reporting

The bank shall include the risk pertaining to remittance and foreign exchange services and other services provided to walk-in customers in its annual ML/TF risk assessment report. The bank shall include the compliance status pertaining to remittance and foreign exchange services and other services provided to walk-in customers in its compliance report.

9.4. Record keeping

The documents of walk-in customer shall also be kept for 5 years from the date of transactions. It includes swift message, KYC form, Citizenship/identity document of customer, passport/visa/plane ticket of the customer and other documents if any. The bank shall keep the records in both physical and digital format to the extent possible.

CHAPTER 10

TERRORISM FINANCINGAND PROLIFERATION FINANCING

10.1. Introduction to Terrorism Financing

Terror financing is a three-step process of collecting, transmitting, and distributing funds for terrorist activities, without catching the attention of law enforcement. This involves raising money, either through illegal or legal channels, and then laundering it through the financial system to conceal its origin and destination. Finally, the laundered funds are distributed to terror cells, which use it to purchase weapons, pay for supplies, or otherwise advance the group's goals.

10.2. Provision related to financing of terrorism

The bank shall take the following measures to discourage and prohibit the financing of terrorism through use of its product, services, network of branches and other channels of distribution:

i. All the customers are screened against sanction list (besides other list) at the on boarding stage and sanctioned person or entities are not allowed to establish business relationship with the bank.

ii. Bulk sanction screening of all the customers are done once in quarter to ensure proper sweeping of customers that are sanctioned post on boarding with the bank.

iii. All the wire transfers, inward as well as outwards, are subject to Swift screening.

iv. Bank doesn't establish any kind of business relationship with persons (legal as well as natural) belonging to nations subject to "Call for Action" by FATF.

v. Accounts of person belonging to FATF declared jurisdictions under increased monitoring will be categorized as high risk accounts and are subject to EDD measures.

vi. The bank will monitor wire transfers against rules that can indicate possible terror financing. For instance, monitoring low value remit transactions with high frequency can trigger potential terror financing transactions.

vii. Any transactions that exhibit terror financing indicators shall be report to concerned authority in a timely manner.

viii. Appropriate due diligence will be conducted by branches and trade finance department to ensure that trade is not used as a means for financing terrorism.

ix. Trade finance transactions with "Abnormal trade routes" will be detected beforehand and appropriate due diligence will be conducted by branch offices and trade finance department to rule out the use of trade for terrorism financing.

CHAPTER 11

MISCELLANEOUS PROVISIONS

11.1. Record Keeping

The Bank shall keep following documents, information and record for minimum 5 years from the date of completion of transaction or event.

- Data/document related to customer/beneficial owner identification, verification, risk analysis, monitoring and other related information along with the date, time and nature,
- Documents/record related to cross border wire transfers,
- Suspicious transaction report,
- Threshold transaction report,
- Data/Document of identified PEPs,
- Data/Document of identified Beneficial Owner,
- Account Opening/KYC/Enhanced CDD forms etc.
- All necessary record on transactions.

Bank will keep all the records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years even afterclosure of account or after the date of occasional transaction. It should be ensured that all the CDD information and transaction records are made available to regulatory authorities when required.

It is understood that digitization is need of the hour. The bank shall explore the possibility of digitizing all its AML related documents, including account opening forms, KYC forms and other documents relating thereto. The following procedures shall be followed in this regard:

- Details of customer as specified in the account opening forms shall be entered in CBS of the bank to the extent possible.
- Bank will take necessary initiatives to ensure that documents submitted by the customers are scanned and stored in digital format.
- Necessary initiatives will be taken to ensure that hard copies document received from regulatory agencies are converted into soft version over time and stored properly.

11.2. Batch Screening

Bank shall conduct batch screening of accounts against sanction lists (UN, OFAC, EU and HMT) and PEP list on a monthlybasis. Besides, the results of batch screening shall be analyzed and closed within a month. The Bank understands that conducting batch screening of accounts nullifies the risk of continuation of business relationships with any customer who gets migrated under sanctioned list post on boarding. Batch screening process shall be closed following a

predefined mechanism and the same shall be well documented by the way of the standard operating procedure.

11.3. Provisions related to AML System

The Bank shall procure and use effective AML system for transaction monitoring and achieving other objectives relating to AML and CFT.

11.4. Ownership

The Bank shall be the owner of its AML system including its server, database, backups and any other up gradation in the system. The IT department of the Bank shall ensure that ownership of the same rest with bank in all respects.

11.5. Database

The database relating to AML system shall be owned by the bank. IT department of the Bank shall devise a mechanism, in consultation with the vendor to appropriately maintain proper back up of the same. IT department of the bank shall also ensure that there is a proper data recovery mechanism in place, in event of any disaster.

11.6. Periodic Assessment

The Bank shall access the performance of the AML system on a periodic basis. Periodic assessment of AML system shall be followed by decision from management committee to continue or replace the system. However, the Board of Directors of the bank shall be the final authority on making decision regarding continuation/replacement of the AML system.

11.7. Remote Access

The bank can provide remote access to the vendor of AML system for the purpose of maintenance. The remote access can be through any of the system/PCs of the compliance department. The bank shall ensure that there is mechanism in place to ensure security of its database/network system while providing remote access.

11.8. Comprehensive KYC Update

The Bank shall maintain full KYC update of all its accounts. Branch offices shall ensure that KYC of all accounts of the branches are updated both in terms of documentation as well as in its core banking system and AML system.

The branch operation department of the Bank shall monitor the status of KYC updates and report the same to management Committee, on a periodic basis, not later than once in a quarter.

11.9. Trade Based Money Laundering Screening Mechanism (TBML)

The Bank is committed to prohibit all forms of TBML if any attempted during day to day banking operations by means of trade. Following provisions shall be noted in this regard.

- Branch offices shall conduct necessary due diligence to identify attempted money laundering by means of trade.
- Trade Finance department shall take reasonable measures to ensure any TBML attempts are identified and prohibited.
- Cases of doubtful TBML attempts should be reported to compliance department for closure and reporting.
- It shall be the duty of branch offices and trade finance department to report to the compliance department the cases of doubtful trade based money laundering for TBML attempts.
- The bank will take necessary measures to ensure that sanction escapes through use of trade channels are not materialized.
- Trade Finance department shall conduct necessary measures to ensure the sanction breaches through trade channels do not get materialized.
- Bank will prepare a list of potential TBML indicators and communicate the same to branch offices through trainings.
- RBBL shall gradually explore the possibility of procuring and implementing vessel tracking system (VTS) so as to minimize the possibility of TBML in international trade transactions.

11.10. Enabling Legal and Regulatory Enforcement

The bank stands committed to ensure that it acts as a catalyst towards legal and regulatory enforcement. The following provisions shall be noted in this regard.

- It shall be the duty of compliance department to notify all the concerned branch offices/departments and/or other stakeholders, the matters which require enforcement, in written form via compliance notice.
- The concerned branch office/provincial office/department shall be responsible to respond to such notification (Compliance notice) and communicate compliance department in written form within stipulated time.
- Upon receipt of response from branch/province office the compliance department shall reply to the concerned enforcement agencies.
- It shall be the duty of all the branch offices to check compliance notice updated in the intranet of the bank, on a daily basis, without failure.
- Branch offices shall maintain a log/record of action taken on each of the compliance notice.

11.11. Code of Conduct

Every staff of the bank shall adhere following code of conduct relating to prevention of money laundering and combating financing terrorism:

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

11.12. Employee Protection

The bank shall ensure that its employees are fully protected from any negative consequences that arise due to suspicious transaction reporting. The bank shall make sure that none of its employees tip off any information related to suspicious transaction to its customers.

In case any employee is found guilty of tipping off information pertaining to STR, the bank shall initiate necessary departmental action against such employee. In addition to this, the bank shall also provide legal support to its employees in case the employee faces any legal problems due to suspicious transactions/activity reporting.

11.13. Departmental Action

If any staff violates the provisions mentioned in this policy/procedure, the Bank shall take departmental action as per the staff service by rule, 2070.

11.14. Amendment to the Policy

The Board of Directors of the bank shall amend the policy and procedures if required upon receiving recommendation of AML/CFT Committee of the Bank.