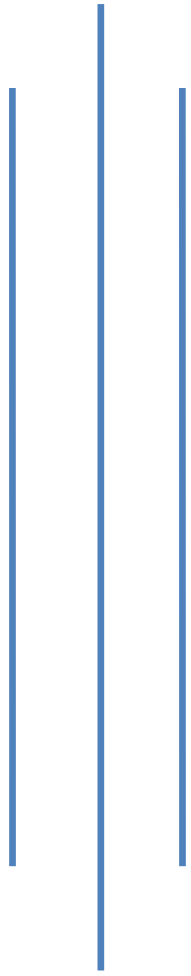
Anti Money Laundering (AML) Policy – 2014

(2nd Amendment on October 2017)



Approval Sheet

Name/ Designation	Signature	Date
Prepared by Surendra Chand Head Compliance	(Original Signed)	
Reviewed & Supported by Bhesh Raj Khatiwada Chief Risk Officer	(Original Signed)	
Supported by Tara Manandhar Deputy Chief Executive Officer	(Original Signed)	
Supported by Ashok Sherchan Chief Executive Officer	(Original Signed)	
Reviewed & Supported by Risk Management Committee	(Original Signed)	
Approved by **Board of Directors**	(Original Signed)	

Date of Approval - November 23, 2017 (BOD # 101)

Table of Contents

1. Preliminary 4
2. Background 4
3. Introduction 5
   - 3.1 Rules & Regulation regarding AML in the country 6
   - 3.2 Guiding Principles 6
   - 3.3 Sources 7
   - 3.4 Relation of Money Laundering & Terrorist Financing 7
4. Objectives 7
5. Roles and Responsibilities 8
   - 5.1 Board of Directors 8
   - 5.2 Senior Management 9
   - 5.3 AML/CFT Compliance Officer 9
   - 5.4 Internal Audit 9
   - 5.5 External Audit 10
6. Customer Acceptance Policy 10
7. Customer Identification Procedures (CIP) 11
8. Customer Due Diligence (CDD) 14
   - 8.1 Applicability 14
   - 8.2 Simplified Customer Due Diligence (SCDD) 15
   - 8.3 Enhanced Customer Due Diligence (ECDD) 15
9. Money Laundering Activities 17
   - 9.1 Impact of Money Laundering 17
   - 9.2 Possible Sources of Criminal Wealth 17
   - 9.3 Stages of Money Laundering 18
   - 9.4 Methods of Money Laundering 19
10. Threshold and Suspicious Transaction 19
    - 10.1 Threshold Transaction Limit 19
    - 10.2 Suspicious Transactions 20
11. Know Your Customers (KYC) & Account Monitoring 21
    - 11.1 Know Your Customer 21
    - 11.2 Customer Account Activities Monitoring 21
12. Risk Based Approach (RBA) 22
    - 12.1 Risk Management 22
    - 12.2 Customer Risk 22
    - 12.3 Country Risk 22
    - 12.4 Product Risk 23
    - 12.5 Other Risk 23
13 PEPS 23
14. Self-Assessment Report 25
15. Staff Training & Reliability 25
16. Know Your Employee (KYE) 25
17. Anti-Money Laundering Risk Analysis 26
18. Automated Screening System 26
19. Sanctions Policy 26
20. Correspondent Banking and relationship with Local BFIs 27
21. Cross Border Correspondent/Wire Transfer 27
22. Resubmission Policy 28
23. FATCA 28
24. Data Protection & Confidentiality 28
25. Record Retention 28
26. Reporting 28
27. Customer Awareness 29
28. Review 29

Anti Money Laundering (AML) Policy – 2014

(Second Amendment on October 2017)

1. Preliminary

a. Short Title: This Policy is called "**Anti Money Laundering (AML) Policy 2014 (Second Amendment 2017)**".

b. **Commencement**: The Policy shall come into implementation immediate of the approval of Board of Directors.

2. Background

Anti-money Laundering (AML) refers to efforts to prevent criminal exploitation of financial system to conceal the location, ownership, source, nature or control of illicit proceeds. Despite the existence of longstanding regulatory and enforcement mechanisms, as well as international commitments and guidance on best practices, BFIs remain challenged to identify and address the gaps and new laundering methods that criminals exploit. According to the rough estimation by International Monetary Fund (IMF) the global volume of Money Laundering could amount to as much as 2.7% of world's gross domestic product, or $ 1.6 trillion annually. Money Laundering is broadly recognized to have potentially significant economic and political consequences at both national and international levels. Despite robust AML efforts in the globe, the ability to counter Money Laundering effectively remains challenged by variety of factors. These include:

- The scale of global money laundering;
- The diversity of illicit methods to move and store ill-gotten proceeds through the financial system;
- The introduction of new and emerging threats e.g. Cyber related financial crimes;
- The ongoing use of old methods e.g. bulk cash smuggling;
- Gaps in legal, regulatory, and enforcement regimes, including uneven availability of international training and technical assistance for AML purposes; and
- The costs associated with BFIs compliance with global AML guidance and national laws.

The Financial Action Task Force (FATF), the international standard setter for Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) efforts, recommends that money laundering should criminalize in line with the Vienna Convention and Palermo Convention. Accordingly like other countries, Nepal also considers the money laundering or smuggling of money and property from or into Nepal as the criminal activities. Sec 3.1 and 3.2 of Asset (Money) Laundering Prevention Act, 2008 (2064, 2nd amendment 2070) of Nepal defines the assets laundering as act of offences.

Since the banks deal with money, it has to be careful to ensure that the banking channel is

not used for money laundering. It is extremely essential to have robust system and procedures for Banks and Financial Institutions (BFIs) to monitor, control or fight against money laundering.

Monitoring and controlling the money laundering activities through the Bank is one of the top priorities for Prabhu Bank to prevent illegitimate activities relating to money laundering and thereby protecting the Bank and financial system from the potential risk posed by such financial crimes.

Thus, the "Anti Money Laundering Policy" has therefore been prepared to prevent the Bank from being used for criminal activities/purposes. Bank intends to conduct business in compliance with all applicable laws and regulations and control criminals from using the products and services for the purpose of money laundering. The Bank intends to extend cooperation to the regulators in order to stop such activities and shall place required operating standards to safeguard the interest of its customers, shareholders, staff, and all the stakeholders as a whole. Skill, care and diligence shall always be applied by all staffs to comply with relevant laws, rules, regulation, code and standards of good practice. Prompt action shall be taken as per this policy to address the issue if any suspicious transaction is identified.

In the regular course of review and revision, the Anti Money Laundering Policy 2014 has been reviewed and revised and brought into implementation with the approval Board of Directors of the Bank.

3. Introduction

Money laundering has been defined metaphorically as "cleaning of the money". Money laundering is the process whereby true origin and ownership of the fund is disguised. In other words, under money laundering process, identity of illegally possessed money is changed so that it appears to have originated from a legitimate source. The source of such illegal income may include terrorism, organized crime, fraud, etc. Money laundering is a major concern to the governments and regulatory authorities all over the world as it poses great threat to the local / international economy and peace.

Banks and Financial Institutions (BFIs) could be used as a medium for channeling the illegal or criminal engaged money into the financial system. The simplest way to clean the illegally earned money is to bring such money into the financial system through different means such

as cash deposits, remittances, e-cards, drafts, electronic transfers, loan repayments and other financial instruments.

3.1 Rules & Regulation Regarding AML in the Country

Asset (Money) Laundering Prevention Act, 2008 (2064) (2nd amendment 2070) is in implementation in Nepal for investigating, controlling and penalizing the money laundering activities. The act is applicable to all concerned engaged in the money laundering and other like illegal activities of remitting, transferring or sending assets from Nepal to abroad or abroad to Nepal. The Government of Nepal has formulated necessary Rules for the implementation of this Act. Nepal Rastra Bank (NRB) has formulated different Directives, Guidelines, Circulars and Notifications regarding the controlling and monitoring of Money Laundering activities through the Bank.

3.2 Guiding Principles

The Bank has taken the following guiding principles against Money Laundering which is, inter alia, to protect the image and reputation of Bank and its employees:

a. Establishing relationship and doing business only with such customers whose status and identity is fully known to the Bank.

b. Having proper system in place for determining, verifying and recording identity, address and business of all customers of the Bank.

c. Having proper system / policy in place for monitoring the relationship on a regular basis to detect any unusual and suspicious transactions and take immediate action in order to correct or control it. For this purpose, risk grading in the accounts/relationship shall be done and monitoring frequency shall be set on the basis of the risk grade of the account/relationship carries.

d. Having proper mechanism in place to scan all kinds of sanctions like: UN Sanctions, UK Sanctions, OFAC Sanctions, EU Sanctions etc.

"Customer" means a person/ entity with which the Bank establishes any kind of lawful business relationship. **"Transaction"** means any act or agreement made in order to carry out any economic or business activities and the term also includes the transactions of purchase, sale, distribution, transfer or investment and possession of any assets.

3.3 Sources

This policy has been formulated based on following domestic and international provisions;

a. Fundamental and prudential norms on AML/CFT.
b. Prevailing Act and Rule of the Country relating to Money Laundering.
c. Circulars and Directives of Nepal Rastra Bank (FIU-Financial Information Unit/NRB-Central Bank of Nepal)
d. Rules and regulations of the Bank
e. Other applicable National & international laws/Treaties/Conventions.

3.4 Relation of Money Laundering and Terrorist Financing

Difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets of organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations. That is known as terrorist financing though having legitimate source.

A technique that is used to conceal the source of money is termed as money laundering with ultimately used for terrorist financing. Funds used to support terrorism may be originated from legitimate sources, criminal activities or both. Both kind of activities are under the Bank's close monitoring and controlling.

4. Objectives

The purpose of this policy is to prevent the entry of illegal money into the financial system. The following objectives have been set while formulating this policy:

a. Having a system in place to verify identity of prospective customers before establishing relationship.

b. Prevent criminal elements from using the Bank for money laundering activities

c. Put in place appropriate controls for detection and reporting of suspicious activities/transactions in accordance with applicable laws/laid down procedures.

d. Set basic guidelines for the staff on AML and KYC to comply with applicable laws and regulatory guidelines.

e. Ensure that the concerned staff members are adequately trained in KYC/AML/CFT

(Combating Financing of Terrorism) laws, policies and procedures.

f. Prevent illicit transfer of money.

g. Prevent use of Banking Channel for criminal activities.

h. Preventing opening of fictitious accounts.

i. Prevent business relationship with shell banks

j. Determine the intended nature and purpose of the business

Above objectives meet the three essentials principles on AML/CFT task of the Bank

a. Proper customer identification

b. High ethical standards and compliance with laws

c. Cooperation with law enforcement authorities, and

d. Policies and procedures to adhere to the statement.

Clarification: A 'Shell Bank' is a bank that has no physical presence in its country of incorporation has no independent assets or operations of its own, but is used by its owners to conduct specific business dealings or maintain control of other companies.

5. Roles and Responsibilities

5.1 Board of Directors (BoD)

- There shall be a Board level committee called "Assets Laundering Prevention Committee (ALPC)" on effective implementation of bank's AML & CFT compliance program. Which shall to assist the Board of Directors in fulfilling its oversight on Bank's compliance with the requirements of AML & its regulations

- Establish, along with senior management and the CRO, the bank's risk appetite, taking into account the competitive and regulatory landscape and the bank's long term interests, risk exposure and ability to manage risk effectively;

- Oversee implementation of the bank's governance framework and periodically review that it remains appropriate in the light of material changes to the bank's size, complexity, geographical footprint, business strategy, markets and regulatory requirements;

- Approve AML & CFT compliance program and ensure its implementation;

- Ensure the compliance with the instruction of FIU- Nepal issued under the its regulations/directives;
- Take reasonable measures through analyzing self assessment report and other periodical report

- Understand ML & TF risk of the bank, take measures to mitigate those risk;
- Ensure compliance of AML & CFT program;

5.2 Senior Management

- Ensure the adequacy of Bank's policy or strategy to prevent ML& TF,
- Emphasize on effective implementation of bank's AML & CFT compliance program,
- Make clear indication of balance between business risk and mitigating measures ensuring compliance at all times,
- Allocate the point of contact for clarification in case of any ambiguity arise,
- Allocate enough human and other logistics to effective implementation of AML & CFT compliance program,
- Be responsive of the level of money laundering and terrorist financing risk where the bank is exposed,
- Ensure the autonomy of the designated officials related to AML & CFT,

5.3 AML/CFT Compliance Officer

- Should be able to act on his own authority;
- Independent on submission of STR/SAR and any document or information to FIU;
- He/she shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by FIU;
- He/she must have access to any information of the bank;
- He/she shall ensure his/her continuing competence.
- Must ensure overall AML & CFT Compliance of the Bank;
- Oversee the submission of STR/SAR or any document or information to FIU in time;
- Maintain the day-to-day operation of the bank's AML&CFT compliance;
- Shall be liable to CEO, Board Committee or BoD for proper functioning of department;
- Shall review and update ML & TF risk assessment of the bank;
- Ensure that corrective actions have taken by the bank to address the deficiency identified by the FIU or NRB.

5.4 Internal Audit

- Understand ML & TF risk of the bank and check the adequacy of the mitigating

measures

- Examine the overall integrity and effectiveness of the AML/CFT Compliance Program;
- Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- Determine personnel adherence to the bank's AML&CFT Compliance Program;
- Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- Assess the adequacy of the bank's processes for identifying and reporting suspicious activity;
- Communicate the findings to the board and/or senior management in a timely manner;
- Recommend corrective action to address the identified deficiencies;
- Track previously identified deficiencies and ensures correction made by the concerned person;
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;

5.5 External Audit

External auditor may also play an important role in reviewing the adequacy of AML & CFT controls by communicating their findings and recommendations to management via a letter, which accompanies the audit report. External auditor would be risk-focus while developing their audit programs and conducts intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits in its audit report.

All Staffs: Compliance is the responsibility of each employee in their normal course of assignment and ignorance shall not be considered as the excuse for non-compliance.

6. Customer Acceptance Policy (CAP)

The primary objectives of a customer acceptance taken by the Bank are:

- To manage any risk that the services provided by the Bank may be exposed to;
- To prevent the Bank from being used, intentionally or unintentionally, for ML/TF purposes; and
- To identify customers who are likely to pose a higher than average risk on Money

Laundering.

Bank shall make the complete understanding upon the existing and prospective customers under the CAP especially on the following:

a. Background

b. Accounts of persons having relationships with banned entities such as individual terrorists or terrorist organizations/FATF Non Cooperative Countries etc. shall not be opened. Watch list / Sanction List/List of Non cooperative Countries published by UN/EU/USA/Other International Authorities shall be one of the sources to identify the same.

c. Information relating to the persons mentioned in (d), and (e) and (f) shall be shared from Head Office, information available in public domain in this regard shall also be considered.

d. Accounts of persons who have been convicted and are in jails can be opened with suitable safeguards decided on case to case basis. However, it should be ensured that banking facilities are not denied, for genuine purposes, merely for the reason that criminal charges have been labeled against them or they have undergone some form of punishment in the past. Therefore, it should be decided on case to case basis.

e. No account in anonymous or fictitious name or account only with numbers shall be opened;

f. No account in the name of any person or entity listed under United Nations Security Council Resolutions (UNSCRs) or their close alliance of the UN on suspicion of involvement in terrorist or terrorist financing activities and proscribed or enlisted by Nepal Government or NRB or FIU-Nepal shall be opened or operated.

7. Customer Identification Procedures (CIP)

Customer identification is an essential part of KYC & CDD measures. For the purposes of this Policy, CIP includes:

7.1 Customer identification procedures require identifying customer and verifying his/her identity by using reliable, independent source of documents, data or information. Thus, the first requirement of Customer Identification Procedures (CIP) is to be satisfied, that a prospective customer is actually who he/she claims to be. The second requirement of CIP is to ensure that sufficient information is obtained on the identity, purpose and nature of their banking relationship. This

would enable risk profiling of the customer and expected or predictable pattern of transactions.

7.2 Extra care shall be taken while opening accounts of various firms and companies belonging to the same group accounts and under no circumstances accounts of shell companies/firms are opened in the Bank.

7.3 All KYC data/documents shall be obtained from customers for verification of their identity and address and other information.

7.4 The customer Identification Procedures are to be carried out at the following stages:

a. While establishing a banking relationship.

b. When relationship manager/officer feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account.

c. Customer identification data shall review before the account is opened.

d. Customer Identification shall also be carried out in respect of non-account holders approaching bank for transaction of walk-in customers for the transaction above Rs.100,000.

e. When signatories change, care should be taken to ensure that the KYC of any new signatories has been updated.

7.5 Identification Process of Ultimate Beneficial Owner:

The beneficial owner is an individual or entity that enjoys the benefits of owning an asset, regardless of whose name the title of the property or security is in.

When establishing relationship with customer, the Bank shall verify the identity of the natural person behind the transactions for example: who owns, controls or on whose behalf the transaction is being done etc. It shall be based on the existing legal and regulatory framework.

Verify Beneficial Owners

Individuals holding proportionate interest of at least 10% or more of the customers through ownership in the intermediate or ultimate holding company.

Natural person who holds a proportionate interest of at least 10% shareholding or exercise effective management control over the Companies.

Beneficial ownership information of legal persons should be determined as follows:

Step 1

i) The identity of the natural persons (if any, as ownership interests can be so diversified that there are no natural persons, whether acting alone or together, who exercise control of the legal person through ownership) who ultimately have a controlling ownership interest in a legal person, and

ii) To the extent that there is doubt as to whether the persons with the controlling ownership interest are the beneficial owners, or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person through other means.

Step 2

Where no natural person is identified under (i) or (ii) above, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

The following are some examples of natural persons who could be considered as beneficial owners on the basis that they are the ultimate owners/controllers of the legal person, either through their ownership interests, through positions held within the legal person or through other means:

Natural persons who may control the legal person through ownership interest

i) The natural person(s) who directly or indirectly holds a minimum percentage of ownership interest in the legal person (the threshold approach).

ii) Shareholders who exercise control alone or together with other shareholders, including through any contract, understanding, relationship, intermediary or tiered entity (a majority interest approach).

Natural persons who may control the legal person through other means

i) The natural person(s) who exerts control of a legal person through other means such as personal connections to persons in positions described above or that possess ownership.

ii) The natural person(s) who exerts control without ownership by participating in

the financing of the enterprise, or because of close and intimate family relationships, historical or contractual associations, or if a company defaults on certain payments.

Natural persons who may exercise control through positions held within a legal person

i) The natural person(s) responsible for strategic decisions that fundamentally affect the business practices or general direction of the legal person.

ii) The natural person(s) who exercises executive control over the daily or regular affairs of the legal person through a senior management position, such as a chief executive officer (CEO), chief financial officer (CFO), managing or executive director, or president

7.6 **Introduction of New Technology:** Bank shall pay special attention to the money laundering threats arising from new or developing technologies and take necessary steps to prevent its misuse for money laundering activities. Bank will ensure that appropriate KYC procedures are duly applied to the customers using new technology driven products.

8. Customer Due Diligence (CDD)

Customer Due Diligence (CDD) combines the Know Your Customer (KYC) procedure, transaction monitoring based on the information and data or documents collected from reliable and independent sources. Bank therefore conducts customer due diligence for two broad reasons:

a. To help the bank to be reasonably satisfied to those customers to know whether they are acting on behalf of another, and that there is no legal barrier (e.g. government or international sanctions) to provide them with the product or service requested; and

b. To enable the organization in investigation, law enforcement by providing available information about customers in due process.

8.1 Applicability: Bank shall apply the CDD measures when it does any of the following:

a. Establishing a business relationship;

b. Carrying out an occasional transaction;

c. Suspecting money laundering or terrorist financing; or

d. Suspecting the veracity of documents, data or information previously obtained for the purpose of identification or verification.

8.2 Simplified Customer Due Diligence (SCDD)

As a mandatory part of the CDD process, Bank shall perform screening of the customer involved against internal and external restriction list and blacklist. Bank shall take reasonable measure to establish relationship weather customer ID is acceptable or not. In due course, the Bank should screen customer using simplified approach of diligence. Such category of customer includes listed companies and public authorities. Prior to applying SCDD, bank has to conduct appropriate testing to satisfy itself that the rejection list or customer qualifies for simplified treatment under this policy.

8.3 Enhanced Customer Due Diligence (ECDD)

The Bank should apply enhanced due diligence measure based on the risk assessment, thereby requiring intensive due diligence for high risk customers. The examples of customer requiring higher due diligence may include;

- Politically Exposed Persons (PEPs)
- Customers doing transactions electronically
- High Net worth Customers (For this purpose, high net worth means net worth having more than Rs.100 mn)
- Customers having basis to believe to have involvement on assets laundering and terrorist activities
- Customers from the high risk countries having high corruption, tax evasion and other criminal activities.
- Customers having large volume of transactions
- Customer of FATF non cooperative jurisdictions
- Customer convicted on predicate offences and financial crime
- Designated Non-Financial Businesses and Professions (DNFBPs) i.e. Casinos, Real Estate Agent, Dealers in precious metals and stones & Lawyers, Notaries, other independent Legal professionals and accountants.

- Customer from UN/US/EU sanctioned countries
- In case of wire transfer through intermediary etc.

Enhanced Customer due Diligence (ECDD) Procedures

- Obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment
- Carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual customer risk assessment
- Commissioning an intelligence report on the customer or beneficial owner to understand better the risk that the customer or beneficial owner may be involved in criminal activity
- Verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from illegitimate source
- Seeking additional information from the customer about the purpose and intended nature of the business relationship
- Senior Management approval to commence or continue the business relation.

High Rank Persons

The Bank shall maintain mechanism to ensure:

- Information about high rank persons so that such database can be linked while opening account, doing any transaction and obtaining customer information on regular interval.
- Mechanism to identify of inclusion / person.

The Bank shall ensure the mechanism to identify the high rank persons:

- Obtain information from the customer
- Collect and maintain the publicly available information.
- Collect and maintain the information available on social media
- Accept and maintain the commercially available information.

- Exclusion of high rank person, as and when occurred.
- Mechanism to identify of family and associated persons of high rank person.
- Mechanism to identify risk according to the position and involvement of high risk

9. Money Laundering Activities

9.1 Impact of Money Laundering

The consequences of money laundering could be extremely serious and can affect the financial system of the country as a whole. All concerned should, therefore, fight against it collectively. A few examples of its effect could be as follows:

a. Volatility of capital flows and exchange rates due to un-anticipated cross border asset transfers.

b. Unexplained, unusual and rapid changes in supply and demand of money.

c. Contamination in the legal financial transactions thereby affecting on whole economy.

d. Increase in illegal activities due to increased cash flow and thereby affecting the society.

e. Liquidity risks to the Bank on account of large deposits / withdrawals in cash.

9.2 Possible Sources of Criminal Wealth

The following, but not limited to, could be the sources of criminal wealth generation:

a. Terrorism, Drug / Human/ Human organs Trafficking, Illegal arms trade, Smuggling, including movement of nuclear materials

b. Other organized crime

c. Corruption/Embezzlement /Tax evasion

d. Counterfeiting, including making of imitation and copies of original products/goods

e. Facilitating illegal immigration

f. Homicide, theft, fraud, forgery including computer/electronic/software/hardware fraud.

g. Offence relating to Nature conservation and forestry, Cooperatives, Banking,

Ancient Monuments/Art and Antique

h. Investment in terrorist activities

i. Offence relating to Foreign Exchange

j. Other Offences prescribed by Nepal Government under any other law or Treaty/Convention to which the Country is a party.

9.3 Stages of Money Laundering

The following are the basic possible steps used for money laundering depends on the available laundering mechanisms and the requirements of the criminal organizations:

1. Placement
2. Layering
3. Integration

Out of the above steps, Money Laundering may occur separately, simultaneously or in phases overlapping one another. In all the three steps, the money gathered illegally is brought into the financial system through financial institutions. The steps are elaborated below in details:

1. **Placement:** The physical disposal of cash proceeds derived from illegal activity could be done through:
    a. Depositing a large amount of cash in numerous small amounts
    b. Investing in shares and other investments products like real state
    c. Mingling of illegal cash with deposits from legitimate business
    d. Exporting Cash
    e. Using illegal cash to buy high value goods, property or business assets
2. **Layering:** Layering is the practice of separation of illegal money from its original source by creating complex layers of financial transactions to disguise the original source of the fund. A few examples are:
    a. A company may route money through its accounts showing the sales proceeds of fake invoices
    b. A customer may incur a large credit card debt from an account and repay the loan from the illegal source.

c. Customer can open a fixed deposit (from the money earned illegally) in a bank and avail loan against it.

d. Cash deposited in overseas banking system

e. Resale of goods/assets

3. **Integration:** Illegal fund generator brings the fund in the system showing the legitimate sources, if the layering process succeeds, so that no one would suspect its origins.

9.4 Methods of Money laundering

a. Legitimate Business/ Commingling of Funds: (Criminals take over and/or invest in businesses that customarily handle a high cash-transaction volume mixing the illicit proceeds with that of the legitimate business).

b. Reverse flip: (A money launderer may find a property seller who agrees to a reported purchase price well below the actual value and then accepts the difference "under the table".)

c. Loan back: (A criminal provides an associate with a specific amount of illegitimate money and the associate provides a "loan or mortgage" back to the criminal for the same amount with all the necessary "loan and/or mortgage" documentation)

d. Frequent account closing

e. Shell Company: (a company that is incorporated but has no significant assets or operations / presence)

f. The use of Conduit Account

g. Underground or Parallel Banking System (Individual or Institution involved massively in informal lending and borrowing giving room to money laundering)

10. Threshold and Suspicious Transactions

10.1 Threshold Transaction Limit

To prevent from the money laundering activities the Bank shall monitor the threshold transaction limit. Currently the cash transactions equivalent to or more than1Million, which includes both LCY & FCY cash transactions however, in case of FCY

transactions, it includes both of cash & wire transfer, in case transactions related to exchange facility of foreign currency worth of more than five hundred thousand on daily basis. Such Threshold Transaction Report (TTR) report shall be submitted within 15 days from the date of transaction to Nepal Rastra Bank, Financial Information Unit (FIU). This is subject to change as per Government & Regulatory Guideline to be issued from time to time.

10.2 Suspicious Transactions

It requires lots of skill, judgment and common sense of the staff of the Bank and system in place to identify the suspicious transactions as it can vary from one transaction to another based upon all the circumstances surrounding the transactions. For example, transaction by one customer may be normal because of the knowledge about that customer while similar transactions by another customer could be suspicious. Many factors are involved in determining whether the transactions are suspicious including the amount of transactions, actual beneficiary of the transactions, capability of the beneficiary earning or receiving that level of amount, type of transactions, frequency of deposits and withdrawal in large amount generally in round figures, destination of transactions, source of funds, etc. Therefore, due care should be given while establishing the account relationship, account should be opened or deposit should be accepted by fulfilling all the procedures relating to KYC and it should be monitored on a regular basis.

General Characteristics of Suspicious Financial Transactions (incorporating the FIU's guidelines on STR)

– Transactions having unclear economical and business target.
– Transactions conducted in relatively large amount cash and/or conducted repeatedly and unnaturally.
– Transactions conducted differently from that of usually and normally conducted by the relevant customer.
– Huge, complex and unusual transaction.
– Transaction deviating from the profile; the characteristics; or the usual transaction pattern of the relevant customer.
– Funds transfer to / from offshore or high risk countries
– Generation of funds from illegal or suspected sources, etc.

11. Know Your Customers (KYC) & Account Monitoring

11.1 Know Your Customer

KYC Manual has been formulated separately as a basic tool to fight against money laundering activities. The key objective of KYC is to establish identity of the prospective customer and verify source of funds which will supplement to achieve the objective of Anti Money Laundering Policy. KYC Manual has set procedures to enable the staff to know about the customer in detail including their identity, addresses, legal status, existing business and likely transactions to be carried out using the Bank and identify the suspicious transactions, if any, carried out.

Primarily, staff at the Customer Service Department or sales staff of deposit or credit products or Branch Managers are responsible for interviewing the prospective customer and obtain sufficient information on the reputation of the client, legitimacy of the business and nature and source of activity expected in the account.

No branch shall establish relationship until the identity of the potential customer is satisfactorily known. Similarly, if any existing customers do not support in furnishing the information relating to KYC, the respective branch should not accept such customer or initiate the process to stop business relationship in case of existing relationship and report such account as suspicious.

Some customers despite having proper source of income hesitate to disclose the source of income and furnish other details. In such a situation, the customer should be educated properly so that they do not feel embarrassed and furnish the information. If required they should be introduced with other senior staff of the Branch or Branch Manager so that they feel comfortable to furnish the information. The staff dealing with customer should get the information by having simple conversation and should not present him / her as if Journalist or Investigator while asking for the information.

11.2 Customer Account Activities Monitoring

A permanent monitoring of customers' accounts/activities shall be put into implementation to detect unusual/ suspicious activities/transactions. Bank shall initiate for the comprehensive automated system monitoring on the transaction monitoring.

12. Risk Based Approach (RBA)

12.1 Risk Management

A risk based approach takes a number of steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risk faced by Bank. Bank shall ensure that its risk management processes for managing money laundering and terrorist financing risk are kept under regular review. Following are the steps applicable under RBA.

- Identify and assess the money laundering and terrorist financing risks that are relevant to the Bank as per Know Your Customer (KYC) manual and regulator guidelines.
- Design and implement measures to manage and mitigate the identified risk,
- Monitor and improve the effectiveness of these controls/measures.

12.2 Customer Risk

Determining the potential money laundering and terrorist financing risks posed by a customer, or category of customers, is critical to the development of an overall risk framework of the Bank. Based on the KYC Manual and regulator guidelines, the Bank shall determine whether a particular customer poses a higher risk of money laundering and terrorist financing or not.

12.3 Country Risk

Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. Country risk is not solely related to the country of origin of a customer. The Bank shall take into account that a customer may have business interests in or relevant links to a country that may signify that the customer should be placed in a high risk category. There are several factor that determine higher risk possession for example,

- Countries subject to sanctions, embargoes or similar measures issued by the United Nations/EU/USA or FATF;
- Countries identified by credible sources (e.g. FATF, FATF-style national authorities or other recognized evaluation bodies) as lacking adequate money laundering laws and regulations;
- Countries identified by credible sources as providing funding or support for terrorist activities and having significant level of corruption or other criminal activities.

12.4 Product Risk

Products and services offered by the Bank may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or services. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Therefore, product design process of the bank shall duly consider AML risk factor while designing the risky product.

12.5 Other Risk

Other factor of risk assessment which determines potentiality of money laundering or terrorist financing which are;

- Geographical location
- Nature of business or Occupation
- Production and nature of production of goods and services
- Nature of transaction and channel of distribution.

Bank shall identify and evaluate the risk arises from above factors with proper consideration of national risk assessment made by regulator and Nepal government.

13. Politically Exposed Persons (PEPs)

Politically Exposed Person is an individual who is or has been given with a prominent public function. PEPs hold positions that can be abused for the purpose of laundering illicit funds.

The term "PEP" generally includes a current or former senior National/Foreign political figure, their immediate family members, and their close associates.

Anti-Money laundering Act defines PEP as a person who holds, or has held at any time in the last 5 year;

High Rank Individuals:-

a. Heads and deputy heads of state or government;
b. Prime Minister, Ministers, deputy ministers and assistant ministers;
c. Senior members of ruling party;
d. Members of parliament and/or national legislatures;
e. Members of the governing bodies of major political parties;
f. Members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional

circumstances;

g. Heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;

h. Head of state-owned enterprises.

i. High-ranking officer of Government (Equivalent to Special class of Government Officer or above)

PEPs Close Associates & Family

Apply ECDD to an immediate family member, or a close associate, of PEPs.

A "close associate" is defined any of the following persons:-

- ❖ Any individual who has joint beneficial ownership of a legal entity, or a legal arrangement, or close business relationship, with PEP;
- ❖ Any individual who has sole beneficial ownership of a legal entity or legal arrangement set up for the actual benefit of PEP.

An "immediate family member" of PEP includes any of the following persons:-

- ❖ Spouse
- ❖ Person who is considered to be the equivalent to a spouse;
- ❖ Cohabitant (domestic partner);
- ❖ Children of the PEP;
- ❖ Spouse of the child
- ❖ Person who is considered to be the equivalent to a spouse of a child;
- ❖ Cohabitant of a child;
- ❖ Parent
- ❖ Any other family member of the PEP who is of a prescribed class

ECDD Procedure for PEPs

Banks identifies whether any of their customer is PEP. Once identified, banks need to apply enhanced CDD measures. Moreover, they need to perform the following-

a. Banks have to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a PEP;

b. Obtain senior managements' approval or Compliance Officer's approval before establishing such business relationship;

c. Take reasonable measures to establish the source of fund of a PEP's account;

d. Monitor their transactions in a regular basis; and

e. All provisions of NRB, FIU Nepal and Assets Laundering Prevention Act/Regulation of Nepal to be complied.

14. Self Assessment Report

In line with the regulatory requirements, bank shall conduct Self Assessment to evaluate itself on a half yearly basis. Self Assessment shall be done through a checklist that is circulated by NRB. After the end of every half year, compliance evaluates the report along with the measures taken by the bank on the issues observed.

15. Staff Trainings & Reliability

The Bank shall ensure full KYC of its employee incumbents and shall not hire staffs that are deemed not reliable or unworthy in terms of AML/KYC requirements.

Every employee of the bank shall have at least basic AML & CFT training that should cover all the aspects of AML & CFT measures in Nepal. Relevant provision of Acts, Rules Circulars, and Guidelines, regulatory requirements, suspicious transaction or activity reporting should be covered in basic AML & CFT training course. To keep the employees updated about AML & CFT measures, bank shall conduct refreshment training programs of its employees on a regular basis.

AML & CFT basic training shall cover the following-

1. An overview of AML & CFT initiatives,
2. Relevant provisions of Money Laundering Act of Nepal,
3. Regulatory requirements as per FIU-Nepal circular, guidelines, directives,
4. STR/SAR and TTR reporting procedure,
5. Ongoing monitoring and sanction screening mechanism.
6. Role of employees having different responsibility such as Teller, CSD officer, Relationship Manager, Operations Incharge, Branch Manager for effective KYC / AML policy compliance.

16. Know Your Employee (KYE)

Lots of instances are come into ahead about the involvement of employees in fraudulent transactions and in most cases in association with customers. This therefore brings in sharp focus the need for thorough checks on employees' credentials and proper screening of candidates to prevent the hiring of undesirables. Policies, procedures, job descriptions, internal controls, approval levels, levels of authority, compliance with personnel laws and

regulations, code of conduct/ethics, accountability, dual control and other deterrents shall be firmly in place. KYE requirements shall be included in the Bank's HR By-Laws.

Before assigning an employee in a particular job or desk, banks shall ensure that the employee shall have necessary orientation on AML & CFT lessons for the particular job or desk.

17. Anti-Money Laundering Risk Analysis

The Bank shall set up a system to assess the level of risk exposure considering product and customer risk from the AML/KYC point of view and derive appropriate security measures from this analysis. Based upon the risk profiling, the frequency and level of monitoring shall be defined.

18. Automated Screening System

For effective implementation of AML and CFT, bank uses the automated screening mechanism that could prohibit any listed individuals or entities to enter into the banking channel. Bank shall operate the system whether they could detect any listed individuals or entities prior to establish any relationship with them. Bank shall ensure that screening has been done on:

a. International relationship or transaction,
b. Opening any account or establishing relationship domestically,
c. For proper screening of UN, OFAC, EU and other sanction list,
d. Transactional review,
e. CDD and PEPs monitoring,
f. Listing & de-listing process

19. Sanctions Policy

The Bank complies with the relevant laws and regulations of country as well as international norms of financial market. The Bank fulfills the requirements set out in such laws and regulations so as to ensure that the Bank is not used to facilitate financial crime. The Bank complies with:

- Applicable regulations of National governments and multinational bodies in relation to financial sanctions; and
- Any other National or International law or regulation applicable to the Bank’s operations.

The Bank complies with the following sanctions measures:

1. Internal list of natural persons and legal entities;
2. United Nations (UN) Security Council consolidated sanctions list
3. EU's consolidated list of persons, groups and entities;
4. US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists:
5. US Department of the Treasury, Financial Crimes Enforcement Network (Fin CEN) list;

   UK HM Treasury (HMT), Office of Financial Sanctions Implementation, "consolidated list of targets".

20. Correspondent banking and relationship with Local BFIs

Special attention must be paid to correspondent banking business and adequate security measures shall be implemented. A level of care has to be given in establishing relationship with local BFIs especially with the following information:

a. Registration documents

b. Operating License

c. Completed AML questionnaire

d. Wolfsburg questionnaire

e. List of Board of Directors & Management Profile

f. Ownership Structure

g. Latest Audited Financial

h. AML Policy & Procedure

i. US Patriot Act Certification

j. Other registration or certification from local or international agencies like: FATCA Status, Wolfsberg questionnaire etc

21. Cross Border Correspondent / Wire Transfer

Before establishing any relationships or cross border payment, the Bank shall check /

conduct screening of the customer status/ transactions with help of automated screening software.

22. Resubmission policy

Once a transaction is rejected due to Sanctions/Money Laundering/Terrorist Financing concerns one should not attempt to resubmit the same transaction after stripping off information. Bank monitors such transactions though are very rare and less in number. The Bank needs to recheck the said transaction & management approval before resubmitting such transactions**.**

23. FATCA

FATCA (Foreign Account Tax Compliance Act) enacted in US related with the tax compliance with the financial assets held outside of United States. Reporting under FATCA is mandatory to U.S. Persons. FACTA rules include extensive criteria that banks will have to use to screen all of their clients to determine which ones appear to be U.S. Persons.

NRB also have brought regulatory provisions for FATCA registration and reporting requirements. Accordingly Bank shall be registered under FATCA do according on information sharing whenever needed.

24. Data Protection and Confidentiality

The information about customer and their transaction obtained during the course of fulfilling AML/CFT internal control is considered as confidential. The employee of the bank should avoid disclosure to another person's the AML/CFT ways and means implemented by the Bank.

25. Record Retention

Records must be kept of all transaction data and data obtained for the purpose of identification, as well as of all documents related to money laundering topics (e.g. files on suspicious activity reports, documentation of AML account monitoring, etc.). Those records must be kept for a period of minimum 5 years from the date of cessation of relationship.

26. Reporting

Reporting is one of the integral parts of AML system to prevent money laundering activities. The Bank shall ensure that the reporting channel for AML purpose is

effectively implemented. The entire employees are responsible to prevent/find out/monitor suspicious activities in their own level and shall report to their respective reporting officer. The reporting officers shall further scrutinize the information and report to AML/KYC Manager at Head Office. If any suspicious activities are found it shall be the responsibility, primarily of Head of AML/KYC Department and then he/she report to the Regulatory Body or FIU-Nepal.

On other hand, Head of AML/KYC shall report to Chief Risk Officer (CRO). CRO is the head of Independent body called Integrated Risk Management Department (IRMD) who shall report to the Board Level Risk Management Committee / Assets Laundering Prevention Committee.

27. Customer Awareness

Banks shall put into practice the proper actions and procedures for awareness program to the existing and prospective customers regarding prevention of money laundering and terrorist financing. At the time of KYC interview and account opening process, details information shall be provided to the customer regarding the AML/CFT. Bank shall also take the mass media under Corporate Social Responsibility (CSR) regarding the money laundering and terrorist financing.

28. Review

This is the Second amendment of Anti Money Laundering Policy, 2014. Policy review shall be conducted whenever it deemed necessary.

The End!

Annexure—A

Indicators of Suspicious Transactions:

1. Transactions having unclear economical and business target.
2. Transactions conducted in relatively large amount cash and/or conducted repeatedly and unnaturally.
3. Transactions conducted differently from that of usually and normally conducted by the relevant customer.
4. Huge, complex and usual transaction.

Red Flags:

Some of the indicators of flagging suspicious transactions or money laundering are outlined below for reference:

1. Cash transactions conducted in an unusual amount from that of usually conducted by the relevant customer.
2. Transactions conducted in a relatively small amount but with high frequency (structuring).
3. Transactions conducted by using several different individual names for the interest of a particular person.
4. Transactions having no conformity with the initial purpose of account opening.
5. Transactions having no relationship with the business of the relevant customer.
6. Transaction amount and frequency are different from that of normally conducted by the customer
7. Fund transfers to and from high-risk offshore financial centers without any clear business purposes.
8. Receipts of fund transfers in several phases and once accumulated the funds are subsequently transferred entirely to other account.
9. Receipts and transfers of funds at the same or approximately the same amount and conducted in a relatively short period (pass-by).
10. Receipts/payments of funds made by using more than one (1) account, either in the same name or a different one.
11. Multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.
12. Unreasonable behaviors of customer when conducting a transaction (nervous, rushed, unconfident, etc.).
13. Frequent change of ownership of same property in unusually short time periods with

no apparent business, economic or other legitimate reason and between related persons.

14. Client wants to re-sell Property shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area.
15. Client wishes to form or purchase a company whose corporate objective is irrelevant to the client's normal profession or activities, without a reasonable explanation.
16. Client gives power of attorney to a non-relative to conduct large transactions (same as above).
17. Use of letters of credit to move money between those countries, where such trade would not normally occur and / or is not consistent with the customer's usual business activity. A Letter of credit is generally resorted to so as to accord more legitimacy to the transaction in order to conceal the real facts.
18. The transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification or that includes changes in regard to the beneficiary or location of payment without any apparent reason.
19. The commodity is shipped to or from a jurisdiction designated as 'high risk' for ML activities or sensitive / non co-operative jurisdictions.
20. The commodity is transshipped through one or more such high risk / sensitive jurisdictions for no apparent economic reason.
21. Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction i.e. trade in goods other than goods which are normally exported/ imported by a jurisdiction or which does not make any economic sense.
22. Trade transaction reveals links between representatives of companies exchanging goods i.e. same owners or management.
23. Unusual curiosity about internal system, control and reporting.
24. Customer gives false information with respect to his/her identity, sources of income or businesses.
25. Use of identification document that is unreliable or alleged as fake such as different signature or photo.
26. Customer is unwilling or refusing to provide information/documents requested by the officials of the relevant reporting entity without any clear reasons.
27. Customer or his/her legal representative tries to persuade the officials of the relevant reporting entity in one way or another not to report his/her transaction as a Suspicious Financial Transaction.
28. 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.

29. Customer tries to maintain close relation unnecessarily or unnaturally with the employees.
30. Customer automatically unnecessarily clarifies or tries to clarify legality of amount or transaction.
31. Any one is earning wealth (including cash) by evading tax, custom duty, land revenue, electricity bill, and water bill, phone bill and any other revenue or government fees.
32. Customer lives unusual lifestyle (both high or low) compared to his/her economic strength, profession/business.
33. No information about the source of income is disclosed or stated or information about the source of income is not satisfactory.
34. If any act or transaction is not found reasonable or is found to have been conducted with irrelevant party or where the transaction has no justifiable purpose.
35. If it is evident that repeated transactions below threshold amount fixed by the FIU for reporting purpose take place.
36. Transaction is related to any person being investigated against or wanted by Police, CIAA, Tax, Revenue Investigation or any other crime investigating agencies in relation to any crime.
37. If reporting institution suspects any transaction relating to the customer against whom the regulatory authorities including Nepal Rastra Bank, Insurance Board, Securities Board, Stock Exchange, Company Registrar, Registrar of Cooperative, Bar Council, Institute of Chartered Accountant of Nepal, etc., have initiated proceedings.
38. The transaction of the customer, where it is known or is evident that any investigation or proceeding has been or is being taken by competent law enforcement or regulatory institution of foreign state.
39. If it is evident that the asset is earned from any offence or illegal as well as unethical activities.
40. Direct or indirect transaction of individual or organization declared suspected to be involved in terrorist or criminal activities by the Government of Nepal or individual or organization listed as terrorist or criminal by United Nation through various resolution or transaction of those directly or indirectly assisting terrorism, terrorist activities, terrorist organization, organized crime, drug offences and any other offences.
41. If transaction seems to be reported based on the news or commentary published in national or international news media about any individual or organization.

42. Transaction related to any person who is involved in suspicious transaction, likely to promote money laundering, terrorist or any other criminal activities or the transaction that appears to be unnatural or suspicious in any manner.
43. If same address or telephone number/mobile number is provided for different unrelated customers.
44. Cross transaction between customers who are not related with each other or any individual transmits or receives amount from unrelated person or business institution's account.
45. 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.
46. Cash is handled unnatural binding or packaging during transaction.
47. Multiple transactions with the people living in the country where AML/CFT regime is poor.
48. Third party is unnaturally, unnecessarily involved or is more active in transaction.
49. Sending money that cannot provide even general information about the recipient of money.
50. If there is unnatural inflow or outflow in the name of the firm, company, organization or person involved in such organizations which are not regulated or where no system of economic inspection is developed.
51. If there is repeated transfer of money to and from the name of foreign individual or the individual living outside Nepal.
52. Transfers or receives amount differently from the way of his professional objective or transfers or receives from different place.
53. Multiple claims for the amount received from one person.
54. One uses different channels to transfer the amount ignoring the usual way.
55. If anyone denies providing identity of the transferor though there are sufficient grounds for him to know such identity.
56. If anyone attempts to transfer or receive amount in a suspicious manner.

Red Flags:

Following are some of the points indicating the **Financing of Terrorism**

1. The parties to the transaction (owner, beneficiary, etc.) are from countries suspected to support terrorist activities and organizations.
2. Use of false corporations, including shell-companies.

3. Inclusion of the individual or entity in the United Nations 1267 Sanctions list, EU Sanctioned List, OFAC Sanctioned List, UK Sanctioned List and more like this.
4. Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
5. Beneficial owner of the account not properly identified.
6. Use of nominees, trusts, family members or third party accounts.
7. Use of false identification.
8. Abuse of non-profit organization.
9. Indicators linked to the financial transactions.
10. The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
11. A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
12. Frequent domestic and international ATM activity.
13. Unusual cash activity in foreign bank accounts.
14. Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
15. Use of multiple, foreign bank accounts.