NCC Bank
नेपाल क्रेडिट एण्ड कमर्स बैंक लि.
Nepal Credit & Commerce Bank Ltd.
Your Business Bank

Anti Money Laundering (AML)/ Combating the Financing of Terrorism (CFT) And Know Your Customer (KYC) Policy, 2018

Nepal Credit And Commerce Bank Ltd.

Bagbazar, Kathmandu

(Approved by Board of Directors Meeting No .670. Dated .7.Feb.2018)

Version History

Version History	Name of Document	Approving Authority	Date of Approval
1st	1. Know Your Customer And Anti-Money Laundering/Combating Financing in Terrorism Policy 2016 2. Customer Due Diligence Procedure (CDD Procedure) 2016	Management Committee	November 28, 2016
2nd	Anti-Money Laundering (AML)/ Combating the Financing of Terrorism (CFT) and Know Your Customer (KYC) Policy, 2018	Board of Director	

Approval Sheet

Particulars	Name and Designation	Signature	Date
Prepared By	Saroj Bhanari- Officer: Operation, Market and Liquidity Risk Management Department Biplav Guragain- AML and CFT Unit		
Reviewed and Recommended by	Binaya Prasad Adhikari Head-Compliance		
Reviewed and Recommended By	Mr. Mukunda Subedi Chief Risk Officer		
Reviewed and Recommended By	Mrs. Bandana Pathak Deputy Chief Executive Officer		
Reviewed and Recommended By	Mr. Ramesh Raj Aryal Chief Executive Officer		
Reviewed and Recommended By	AML Committee		
Board of Directors			

Table of Contents

1. Overview of Money Laundering and Terrorist Financing

1.1 Introduction

The fight against Money Laundering (ML) and Terrorist Financing (TF) has become the topmost priority over the world. ML and TF pose the risk to the soundness and stability of financial institutions and financial systems of the Country.

Money laundering in Nepal is an emerging problems and challenges. Nepal has consistently been maintaining the robust Anti-Money Laundering (AML), Preventing Terrorist Financing and Know Your Customer practices. Laws and Regulations have been promulgated to address the Prevention of Money Laundering like Assets (Money) Laundering Prevention Act, 2008 (Second Amendment 2015), Asset (Money) Laundering Prevention Rules, 2016 and various directives from regulatory authorities.

Nepal Rastra Bank has advised to follow robust system and procedures for customer identification procedure for opening of accounts and monitor transactions of suspicious nature for the purpose of reporting the same to Financial Information Unit of Nepal (FIU-Nepal). Unified Directive- 2074 issued by NRB through Directive no 19 has been issued in the context of Anti Money Laundering (AML) standards and on Combating the Financing of Terrorism (CFT). Banks and Financial Institutions have been advised to ensure that a proper policy framework on AML, CFT and KYC measures is formulated and put in place with the approval of their Board.

Nepal Credit & Commerce (NCC) Bank Limited is committed for the compliance of KYC, AML and CFT in line with the prevailing Laws, Regulations, Regulatory Directives and other international standards and best practices. This Policy has been formulated in view to prescribe the standards in KYC and measures to fight against ML and TF.

1.2 Objectives

The objective of the Policy is to prevent the Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable the Bank to know and understand their customers and their financial dealings better and manage their risks prudently. Basic objectives of the policy are as follows.

- Establish standard procedures regarding identification of individuals, firms, companies and other entities while establishing relationship.
- Establish proper procedure to prevent criminal activities to be sued for money laundering activities.
- Enable the Bank to know/ understand the customers and their financial dealings, which in turn would help the Bank to manage risks prudently.

- Put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws and other laid down procedures.
- Monitor transactions for identifying the appropriateness of customers' transactions with their profiles.
- Ensure that the staff members are adequately trained in KYC and AML/CFT laws, policies and procedures.
- Ensure that staff members comply with Anti-Bribery and Anti-Corruption measures of the Bank

1.3 Scope and Applicability

This Policy is applicable to all departments, branches, units, subsidiary companies and other external agencies which are connected with AML and KYC related functions.

This Policy is intended to supplement the Acts, Rules, Regulations, Guidelines and Directives on Prevention of Money Laundering issued or to be issued time to time. However, provisions under the said Acts, Rules, Regulations, Guidelines and Directives shall prevail in case of any contradictions. Similarly, Directives or Guidelines of NRB and FIU-Nepal issued from time to time with regard to KYC and AML/CFT shall also prevail over and be integral part of this policy. Therefore, this policy should be implemented in conjunction with prevailing Acts, Rules, Regulations, Guidelines and Directives.

1.4 Definitions

1.4.1 Money Laundering

Money laundering is the process by which illegal funds and assets are converted into legitimate funds and assets. In money laundering illegal or "dirty money" is put through a cycle or series of transactions or "washed" to convert the money to "clean" or "legal" money.

The proceeds of crimes such as drug trafficking, smuggling, kidnapping, gambling, robbery, counterfeiting, tax evasion, misappropriation of public funds, bribery etc. are converted into legitimate funds through series of financial transactions making it impossible to track back the origin of funds. Most often, BFIs are used for this process. Money launderers use various method and technique to conceal dirty money such as using shell company/bank, offshore bank, structuring, hawala, currency exchange, valuable commodities/assets, gaming activities, non-profit organizations, nominees and gatekeepers etc.

Money Launders use various techniques for laundering funds; however, there are generally three stages in the process:

Stages of Money Laundering

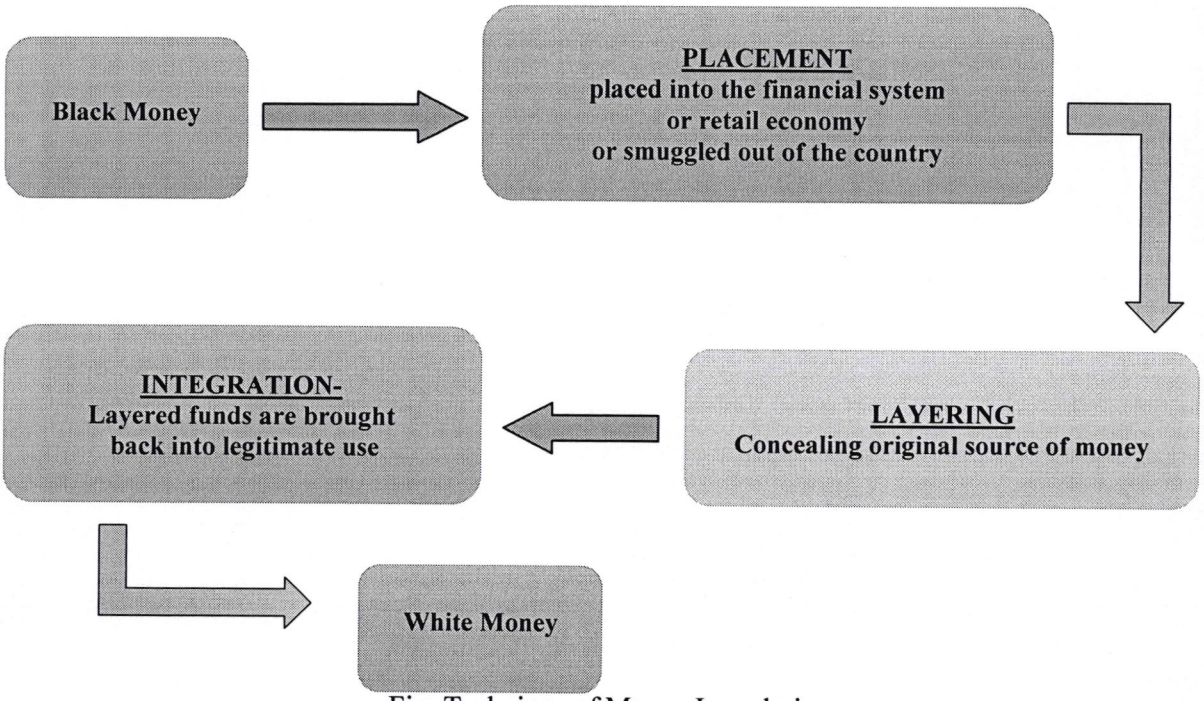

Fig: Technique of Money Laundering

i. Placement

Illegal funds or assets are first brought into the financial system. This placement makes the funds more liquid. Money launders place illegal funds using a variety of technique like, depositing cash into bank accounts or purchasing insurance products and using cash to purchase assets. The money launders insert the illicit money into a legitimate financial system.

ii. Layering

To conceal the illegal origin of the placed funds and thus make them more useful, the funds would be moved, dispersed and disguised. This activity is known as "layering". At this stage, money launders use many different techniques to layer the funds like, using multiple banks and accounts, creating complex nature of financial transactions, having professional act as intermediaries and transacting through corporations and trusts. This helps the launders to disguise the origin of the funds.

iii. Integration

In this stage the money re-enters the mainstream economy in the legitimate looking form. It involves placing the laundered proceeds back in the economy under the veil of legitimacy. It would be very difficult to trace the original source of the money if there is no proper documentation in the previous two stages of money laundering. The funds seem to be cleaned and can now be made available for investment in legitimate or illegitimate business.

1.4.2 Financing of Terrorism

Financing of Terrorism refers to activities of providing or collecting legal or illegal funds or other supports, directly or indirectly, unlawfully and willingly, with the intention or knowledge to use or be used to carry out terrorism, terrorist or terrorist organization, terrorist activities or associates.

The Primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the source of the money but to conceal both the financing and the nature of the financed activities.

A significant 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.

1.4.3 AML/CFT Risk

Bank exposes mainly the Business Risk and Regulatory Risk on AML/CFT and KYC.

Business risk is that the Bank is used for money laundering and terrorist financing. Banks assess the following risks in particular on mitigating the business risk:

- Customer Risks
- Products or Services Risks
- Business Practices and/or Delivery Risks
- Country or jurisdictional risks

Regulatory risk is associated with not meeting all obligations of bank under the Money Laundering Act, Rules, Regulations and Directives. Regulatory obligations are in general failure to report STR/SAR, unable or inappropriately verification of customers and lacking of AML & CFT program etc. It is unrealistic that the Bank would operate in a completely ML & TF risk-free environment. Therefore, the Bank identifies the ML & TF risk it faces, and work out the best ways to reduce and manage that risk.

1.4.4 Customer

For the purpose of KYC Norms, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with the Bank and it includes a person who is engaged on behalf of customer.

2. National and International Initiatives on AML and CFT

2.1 International Agencies, Authorities and Conventions

Various international authorities and entities are working for the Anti Money Laundering and Combating the Financing of Terrorism. Some of the active entities on international level are:

a. Financial Action Task Force (FATA)
b. Asia Pacific Group on Money Laundering (APG)
c. Caribbean Financial Action Task Force (CFATF)
d. The council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures
e. The financial Action Task Force on Money Laundering in South America
f. Middle East and North Africa Financial Action Task Force
g. Eurasian Group
h. Eastern and Southern Africa Anti-Money Laundering Group
i. Intergovernmental Action Group against Money-Laundering in West Africa
j. The International Monetary Fund (IMF)
k. The World Bank
l. Foreign Account Tax Compliance Act (FATCA)
m. The United Nations (UN), The Vienna Convention, The Palermo Convention for Drug Trafficking

2.2 National Agencies and Authorities

In Nepal, basically following agencies and authorities are working for AML/CFT and KYC.

a. The Nepal Rastra Bank (NRB)
b. Department of Money Laundering Investigation (DMLI)
c. Financial Information Unit Nepal (FIU-Nepal)
d. Commission for the Investigation of the Abuse of Authority (CIAA)
e. Nepal Police
f. Revenue Investigation Department (RID)
g. Tax, Customs and Immigrations Authorities
h. Prosecutors and the Courts
i. The Securities Board of Nepal (SEBON)

j. Insurance Board

k. Department of Cooperatives

2.3 National Legal Framework

Nepal Government and Nepal Rastra Bank have issued various acts, rules, guidelines and directives for regulating the AML/CFT and KYC. Some of those key regulations are as follows:

a. Assets (Money) Laundering Prevention Act, 2008 (Second Amendment 2015)

b. Asset (Money) Laundering Prevention Rules, 2016

c. Directive on Assets (Money) Laundering and Combating Financial Terrorism issued by Nepal Rastra Bank

d. Guidelines for Detecting Suspicious Transactions

e. Guidelines for Threshold Transactions Reporting

f. Directives/Guidelines issued by FIU- Nepal (Directives to implement UNSCR (United Nations Security Council Resolutions) 1267 & 1373

3. Functional Structure

Independent and competent functional structure is established for monitoring and controlling the ML, TF and KYC. The functional structure on AML/CFT and KYC is as below.

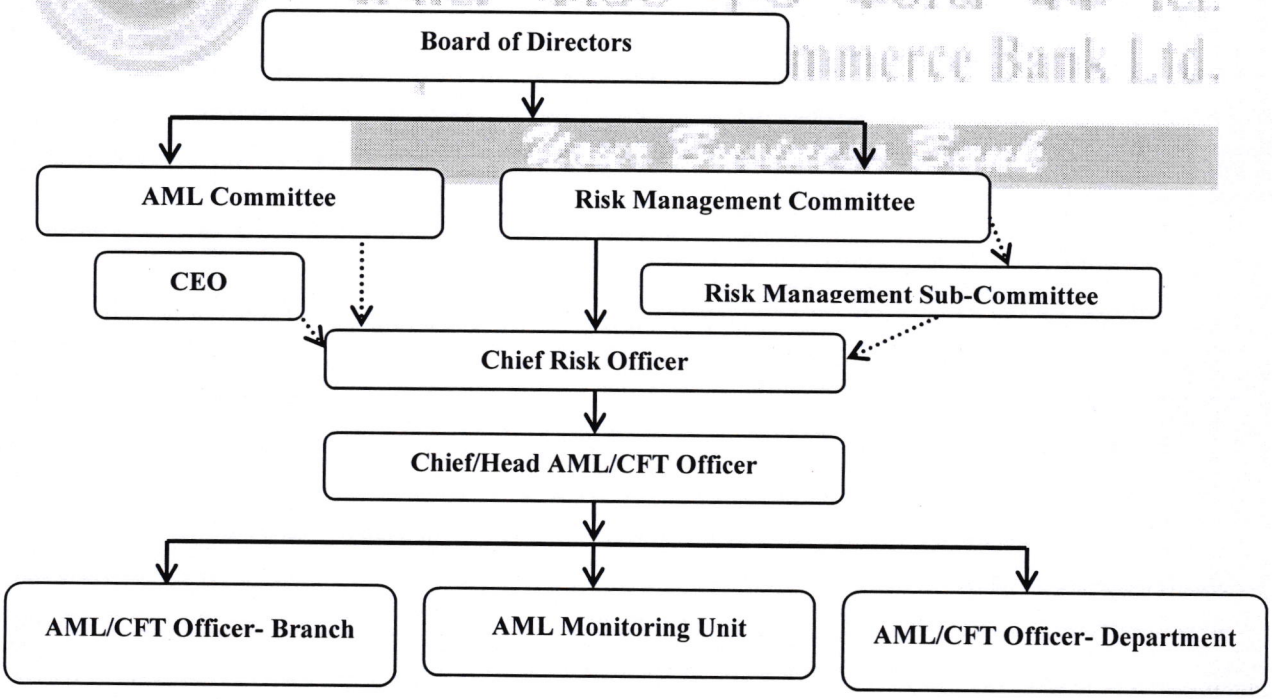

Fig: Functional Structure of AML/CFT and KYC

3.1 Board of Directors (BoD)

The Board of Directors shall be responsible for reviewing/approving the policy document on prevention of money laundering & financing of terrorism. Board of Directors of the Bank discuss

on functioning and effectiveness on AML, CFT and KYC at least on quarterly basis and instruct for needful improvements.

3.2 Risk Management Committee

Board level Risk Management Committee closely monitors the overall functionality of AML/CFT and KYC in the Bank. The Committee is responsible for oversight and policy-setting of risk management activities and communication to the Board of Directors. The Committee proactively reviews AML/CFT and KYC standards and provides instructions/recommendations to improve in the Bank.

3.3 AML Committee

Board level Anti-Money Laundering Committee works for closely monitoring the practices of AML, CFT and KYC practices in the Bank. It advises to the Board for needful improvements on policies and practices. The Committee is primarily responsible for ensuring the adequacy of developed/updated policy and procedures in the Bank. The Committee shall review the AML/CFT functional structure, segregation and performance of duties and responsibilities of AML officers, adequacy and effectiveness of reporting format, suspicious and threshold transaction screening methodologies and provide the valuable feedback/suggestion for update and revision.

3.4 Chief/Head- AML/CFT Officer

Bank assigns the responsibility of Chief/Head- AML/CFT Officer (AML Officer) to a managerial level staff having adequate level of knowledge on overall banking activities. AML Officer assumes overall responsibility for co-coordinating the identification and management of the Bank's AML/CFT and KYC risk, implementing the policy and guidelines in the Bank and for supervising the activities of other functional staffs.

The AML Officer has access to all units, departments, branches and teams for the purpose of discharging assigned responsibilities, including the conduct of autonomous and independent functions.

Name, designation, address, qualification, contact number, email address of the AML Officer shall be provided to FIU-Nepal. General roles and responsibilities of AML Officer are as below:

- Function as a focal point to perform tasks in accordance with the Act, Rules and the Directives.
- Formulation of policies, procedures and system for implementation of Act, Rules and Directives.

- Analysis of the unusual and Suspicious Transaction Report (STR) as identified or received from branches and departments. Submit Transaction Threshold Report (TTR), Suspicious Transaction Report (STR) and other reports to FIU on time as per regulatory requirement.
- Ensure that new policies, rules, procedures and processes or changes to existing ones related with AML/CFT are effectively communicated and implemented throughout the Bank.
- AML Officer shall prepare the report on the compliance of AML/CFT Act, Rules, Directives issued by NRB on quarterly basis.
- AML Officer ensures that all staff members receive appropriate training on money laundering on regular intervals.
- Train staff through awareness raising activities in regard to Know Your Customer (KYC), Anti-Money Laundering (AML), Bribery, Corruption, Conflict of Interests and ethical matters and act as a contact point within the Bank for queries from staff members in respect of AML/CFT and KYC.
- AML Officer recommends for the disciplinary action in case any staff does not co-operate and provide the document / information as demanded while implementing the policy, prevailing acts, rules and directives
- For accomplishment of any task during implementation of this policy, AML Officer can seek help from other department, expert advice from executives; ask for necessary information and documents at any point of time.

3.5 AML Monitoring Unit

An independent AML/CFT monitoring unit works under the supervision of AML Officer. The Unit is responsible for the monitoring and compliance of all regulatory and internal requirements in the context of AML, CFT and KYC. In general, the unit is responsible for the following activities.

- Maintain database of name, address and other available details of Politically Exposed Persons (PEPs), High Ranking Officials, Influential Persons, Persons/Institutions believed to be involved in terrorist activities (as announced by Government of Nepal, OFAC, UN, HMT, EU and / or as circulated by regulatory authority), persons/entities enquired by various statutory investigative authorities, customer having adverse media information, persons who are investigated/penalized for involvement in bribery and corruption, customer with whom bank is unable to communicate even after applying all available medium, blocked accounts etc.

- Receive the STR and TTR report from the branches, analyze it, obtain the required documents and forward to AML Officer. Analyze centrally the suspicious transactions or activities and report as needed.
- Prepare checklist for self-assessment of branch, Bank Self-Assessment Questionnaire, review it and reports to regulatory body as per requirement.
- Prepare offsite data collection form issued by NRB and report to Bank Supervision Department.
- Aware the branches and staffs prevailing trends and symptoms of ML and TF and advises the needful actions for prevention and controlling of ML and TF.
- Other functions as needed for the compliance of AML Policy, KYC Policy and Procedural Manuals of the Bank along with the NRB Directives related with AML, CFT and KYC.

3.6 Branch and Department AML Officer

Head of Department, Branch Manager or Unit Head work as the AML Officer for their respective department, branch or unit. They are the focal person for implementing this policy in their Department, Branch or Unit, and shall be responsible for monitoring and reviewing the activities for controlling the money laundering and terrorist financing. They shall co-ordinate with Chief/Head- AML/CFT Officer for the issues identified. The AML/CFT Officer conducts with the roles and responsibilities as below:

- To ensure that the Policy is properly implemented.
- To ensure that all staff at their department, branch or unit has undergone training in Anti Money Laundering, Combating the Financing of Terrorism and Know Your Customer.
- To file suspicious transaction/activity report to AML/CFT Monitoring Unit.
- Liaise with Chief/Head- AML/CFT Officer and AML Monitoring Unit on continuous basis.

3.7 All Staffs

All staff members of the Bank are responsible to comply with the Bank's Policy, Procedures and Guidelines. Staff shall be well versed with Bank's policies and procedures on AML/CFT and KYC.

4. Know Your Customer

Know Your Customer (KYC) is the process of verifying the identity of customers and ascertain relevant information by using reliable and independent document & information before establishing business relationship. KYC enables the Bank to know/understand their customers and their financial dealings. KYC becoming much more important globally to prevent identity

theft, financial fraud, money laundering, terrorist financing, bribery and corruptions. Bank shall not establish business relationship for which customer identification and KYC is not performed.

4.1 Timing of KYC

Bank applies the KYC procedures on the following timing and stages.

- New Relationship Establishment
- Account Opening
- One Off Transaction and Transaction exceeding the specified limit
- Fund Transfer or Wire Transfer on electronic means
- When the Bank find that existing documents are incomplete or are suspected on its trueness
- Suspected to have engaged on Money Laundering or Terrorist Financing
- Transactions of High Risk Accounts
- High Value and Suspicious Transaction
- Customer profile does not meet with volume of transaction
- Beneficial Owners and Related Parties
- Changes on Signatories, Mandate Holders, Beneficial Owners
- Other conditions as mandated by regulatory authorities

4.2 Customer Acceptance Policy

Bank applies the procedures of screening and accepting the customer under the Customer Acceptance Policy (CAP). Bank prescribes the customer acceptance procedures considering the matter as mentioned below.

a. Customer Background

b. Accounts of person or entity whose place of origination is located in sanctioned countries as declared by Nepal Government, OFAC, UN, HMT, EU, US etc.

c. Relationship with individual with known criminal background or high risk entities such as individual terrorist or terrorist organizations shall not be established.

d. Bank shall consider the risk profile of the persons and open the account with suitable safeguards decided on case to case basis. Additional safeguarding measures shall be applied while opening account of person or entities with high risk profile such as Politically Exposed Person (PEP), Person in Influential Position (PIP), High Ranking Officials etc.

e. 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 or enlisted by Nepal Government or NRB or FIU-Nepal shall not be opened. If already opened, those accounts shall be blocked and reported to the concerned authority.

f. Relationship shall not be established with person / entity barred by law of the land to avail banking facilities.

g. No account shall be opened in the name altering from the primary identity document, anonymous or fictitious (Benami) name(s)/entity(ies), account only with number or blank names.

h. Relationship shall not be established with shell companies and the entities that have relationship with shell companies.

i. Relationship shall not be established with the persons or entities which have not given the adequate documents for KYC purposes.

j. If the existing relations come under the above given restricted scopes, the relationships shall be terminated.

k. Other Risk Indicators

The procedures shall comprehensively categorize the customer as restricted customer, high alert customer and normal customer for their acceptance to be customer or execute transactions. Decision making for customer acceptance shall not be outsourced.

4.3 Customer Identification Policy

The Customer Identification Policy **(CIP)** enables the Bank to form a reasonable belief to know the true identity of each customer. CIP specify about identifying information that will be obtained from each customer on account opening or establishing relationship or executing the transactions.

Bank shall take reasonable step to obtain sufficient evidence of identity, to be able to establish the true identity of the customers / prospective customers. Bank develops the customer identification procedures incorporating the information and matters as guided below.

a. Reliable and independent source of documents, data or information shall be collected for identifying customer and verifying his/her identity so as to be satisfied his/her identity.

b. Screening of customers shall be done on the basis of basic information such as customer's addresses, relationships, occupations and sources of income/fund, expected income, expected turnovers/transactions and purpose of establishing a relationship with the bank along with the thumb impression.

c. Bank shall verify the identity of the true and beneficial owner of the account by obtaining the document supporting ownership and control structure of the customer who have ultimate control over the management and decision making or on whose behalf the transaction has been done.

d. Risk profiles of customer shall be assessed on the basis of documents/information provided to the Bank. The international sanctioned list, sanctioned list from country's authorized authorities, internal database for PEPs, HRO, PIP, Adverse Media, Rejected List and other relevant database shall be used for the purpose of accessing customers risk profile.

e. Bank shall obtain the additional identity verification document for the person or entities belonging to high risk profile. Bank shall obtain additional document such as AML/CFT questionnaire, policy and procedure relating to AML/CFT and KYC so as to ensure that they are fully compliant with the required KYC and AML/CFT standards from correspondent bank.

f. Bank shall reconfirm the identification information/document by physically verifying the address, interviewing the prospective customer if it deemed necessary.

4.4 Walk-In / One-Off Customer

Walk-In / One-Off Customer are those customers who visit the Bank occasionally for the banking service without maintaining bank account with the Bank. Bank shall not deal with such Walk-In / One-Off customer in normal circumstances. If the transaction is executed, Bank follows the customer identification procedures with the minimum information of Name, Address, Date of Birth, Registration Date, Father's or Mother's Name, Nationality and identification documents as prescribed by the Bank.

4.5 Non-Face- To- Face Customers

Non- face- to- face customers are those customers with whom the Bank does not have direct interaction at the time of opening the account or executing transactions. Bank does not open and operate the account of non-face-to-face customers. Non-face-to-face transactions shall be taken with the high priority for transaction monitoring and surveillance whether they are free from money laundering or suspicious natures.

4.6 Politically Exposed Persons, High Ranking Officials, Influential Persons

Politically Exposed Persons (PEPs), High Ranking Official (HRO) and Influential Persons (IP) are the persons who hold key positions or status politically, government or on the areas which have extensive influential. Bank maintains the database of PEPs, High Rank Officials and Influential Persons and check while establishing relationship with the customer. Customer under

the PEPs, HRO or IP shall be categorized under High Risk and shall be conducted Enhanced Customer Due Diligence (ECDD). The relationship shall be established only after the approval of Head of Compliance on the request of respective business head or Chief Operating Officer (COO) of the Bank. Transactions of those customers shall be screened and monitored closely on enhanced way.

4.7 Borrowers

Bank shall obtain all necessary documents to understand and identify the loan clients. Special attention shall be provided to understand and identify whether there exist beneficial owner and loan has been borrowed on behalf of others by analyzing information of subsidiaries, parent company, third party guarantors, multiple banking credit facility and individual owners. Account and transaction of all loan clients shall be reviewed on regular basis and immediately when unexpected repayment of overdue credit without any plausible reason is made. Special attention shall be given while reviewing the cash transactions. Bank shall provide risk grading to its loan clients according to the volume, nature, source of income and area of utilization of loan.

4.8 Beneficial Owners

Beneficial owner is the person who ultimately owns or controls firm and/or a person on whose behalf the transactions or account is being conducted, and include person or persons who exercise ultimate effective control over a person, firm or company. Bank takes the identity of all beneficial owners for the KYC purpose. Beneficial owner shall also be assessed from risk point of view whether it falls under high risk or low risk. Principal account shall be risk graded as high risk if the beneficial owner falls under high risk. Bank prescribes the procedural for identifying and taking identifications of the beneficial owners.

4.9 Risk Assessment

Bank classifies the risk of customers and transactions in the context of associated risk on money laundering from regulatory and internal perspective. The risk is based on the risk perceptions associated with the parameters comprising a customer's profile and the level of risk associated with the product and channels being used by the customer. Risk assessment procedures of the Bank shall incorporates the measures of customer classification based upon the key influencing factors such as geographical, occupational, professional, sector, customer type, product or service type, nature of transaction and as identified by. Risk categorization shall not be disclosed to the customers. Risk shall be classified as High Risk, Medium Risk and Low Risk.

In general, following broad approach shall be adopted for risk categorization,

a. Customer constitution: Individual, proprietorship, partnership, private limited, etc.

b. Business segment: Retail, Corporate, etc.

c. Country of residence/ Nationality: Whether Nepal or any overseas location or foreign national.

d. Product type: Business account, Salary account, NRN account etc.

e. Economic profile: NGO, INGO, Public Limited, Money Transfer etc.

f. Account status: Active, inoperative, dormant.

g. Presence in regulatory negative/PEP/defaulter/fraudster lists.

h. Suspicious Transaction Report (STR) filed for the customer.

i. AML/CFT and KYC alerts, etc

4.10 Know Your Employee (KYE)

Know Your Employee (KYE) procedures support the Bank on understanding the existing and prospects employee's background, conducts, risk profiles and overall acceptability as per the internal policy of the Bank. Bank put the KYE practices with standard set of information and documents. Employee's transactions and profiles shall be assessed periodically from both money laundering and staffs conduct perspectives.

5. Customer Due Diligence and Transaction Monitoring

Customer Due Diligence (CDD) is the process of ensuring that Bank has adequate controls and procedures in place so that all customers, being dealt with, or with whom a relationship is established, are adequately known to the Bank.

5.1 Normal CDD

CDD comprises the tasks of periodic update of profile/information/documents of customer and beneficiary. Bank holds the right to suspend or terminate the relationship while conducting CDD

5.2 Enhanced Customer Due Diligence (ECDD)

Bank applies ECDD for customers that are likely to pose a higher risk from money laundering or terrorist financing perspectives specially the following customers/persons:

a. High net worth persons,

b. PEPs, High Ranked Officials, Influential Person and their family members

c. Non- Face- To- Face customers

d. High cash transactions customers

e. Customer doing transaction frequently through electronic media

f. Suspicious customers

g. Customer from those country which are highly vulnerable to corruption, tax evasion and other criminal activities

h. Other high risk customers/accounts

In general, following measures shall be applied while conducting the ECDD.

a. Examine the background and objectives of complex, large and unusual transaction.
b. Identify the cause of large volume transactions based upon the objectives and business of the customer.
c. Identify the beneficial owner or controlling person of the customer and obtain additional documents when needed.
d. Obtain the approval of higher authority whether to continue or discontinue the relationship with the customer.
e. Determine the limit of transactions.
f. Examine the documents whether these are updated or not.
g. Prepare the ECDD report, record it permanently and provide the report for audit purposes.
h. Every transaction of high risk accounts to be examined from AML and CFT perspectives.

5.3 Frequency

Bank conducts the Customer Due Diligence (CDD) of low risk account every Three Years. CDD of medium risk account shall be conducted on every Two Years. Bank conducts the Enhanced Customer Due Diligence (ECDD) for the high risk accounts annually. Though having defined period, CDD or ECDD shall be conducted as and when required by different situations specially while identifying suspicious transactions.

5.4 Ongoing Monitoring

Ongoing monitoring is essential for understanding of customers' activities and an integral part of effective AML/CFT systems. It helps the Bank to know the customers and to detect unusual or suspicious activities. Bank shall continuously monitor its business relationship with a customer by:

a. Reviewing from time to time the documents, data and information relating to the customer to ensure that they are up-to-date,
b. Monitoring the activities (including cash and non-cash transactions) of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds,
c. Identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF.
d. Monitoring the transactions and purpose of cards issued and electronic devices used in foreign countries and foreign cards used in Bank's system.

6. Assets Block of Sanctioned Persons / Firms/ Companies

Bank maintains the data base of the persons, groups and organizations who are involved in terrorist activities or manufacturing and supply of illegal weapons of mass destruction or financing on such activities as published by Nepal Government and The United Nations Security Council. Bank shall not establish the relationship with those sanctions persons or entities and if relationship is already established, it shall be blocked or freeze immediately. Bank blocks the assets/fund of such person/organization/group along with followings if found the name in the sanctioned list:

- All assets/funds which are controlled directly or indirectly by such person/organization/group in single or joint ownership
- All increment in assets/funds in respect of above
- All assets/funds of those entities which are working in respect of / instruction of such sanctioned entities
- No transaction shall be allowed in such blocked account and no benefit through such assets/fund will be availed to such person/group/organization.

7. Correspondent Banking

Bank implements the risk based due diligence in the context of AML/CFT of the correspondent bank while establishing relationships. Bank obtains the periodical updates of AML/CFT status of respondent bank through questionnaire and other means of reliable information. Bank monitors the transaction with the respondent banks on an ongoing basis. If the Bank found that respondent bank does not have adequate measure of AML/CFT, the relationship shall be stopped. Basic information that has to be taken on correspondent banking relationship would be as below:

- Complete KYC procedures of the respondent bank.
- Update adequate information of the business and activities of the respondent bank.
- Update the information of the respondent bank in regard to the social strength, supervisory standard, and fine on non-compliance of AML/CFT or KYC.
- Assess the adequacy of policies and procedures of the bank.
- Ensuring that the respondent bank does not allow or have established the relationship with shell bank or shell entity.

8. Shell Bank / Shell Entity

Shell bank /entity mean "a bank / entity that has no physical presence in the country in which it is incorporated and licensed. Bank does not establish the business relation with shell banks / entities and/or with other entities which have relationship with shell bank/entities.

9. Anti- Bribery and Anti-Corruption

Bank strictly prohibits the bribery and corruption from Bank staff members, board members and customers as well. Bank does not entertain the customer transactions which are from bribery and corruption activities. Transactions screening would be focused on anti-bribery and anti-corruption on the customer accounts and report as suspicious if found connected with bribery and corruption. Employees shall not demand or accept any gifts from third parties and shall not engage in any behaviors that might be interpreted as such. One of the topics of training on AML/CFT and KYC would be the Anti-Bribery and Anti-Corruption measures.

10. Transaction Monitoring and Reporting

Transaction Monitoring is a critical and resource intensive component of the effective Anti-Money Laundering (AML) program. To the best possible, Bank uses the automated and most reliable software for transaction monitoring, risk indicator flagging and reporting on daily basis or in real-time. Bank primarily conducts the two types of transaction monitoring and reporting as Threshold Transaction Monitoring and Suspicious Transaction Monitoring. The general possible areas of transaction monitoring would be transaction type, frequency, unusually large amounts, geographical origin/destination, changes in account signatories etc.

10.1 Threshold Transaction Reporting (TTR)

Bank monitors the cash transactions as per the threshold as guided by the Nepal Rastra Bank. Bank may set the transaction threshold for its internal screening purposes. Transactions within the scope of TTR shall be reported to FIU-Nepal within the prescribed time period.

10.2 Suspicious Transaction or Activity Reporting (STR)

Suspicious Transactions are those transactions which are abnormal in general economic, commercial and business practice. FIU-Nepal also declares the nature of suspicious transaction based upon the prevailing market trend and situational condition. Bank conducts the transactions and customer activities monitoring on continuous basis and report instantly the STR if found. Suspicious transactions report shall be preserved for at least five years.

10.3 Wire Transfer / Electronic Transfer

Wire and electronic transfer shall closely be monitored for assessing the risk of money laundering. Bank defines the limit of electronic transfer and electronic services in the context of AML/CFT. Bank does not accept the cross–border as well as domestic wire transfer request of the customer incase required information / document is not provided / available for both originator & beneficiary. Customer identification procedures are applied while accepting wire transfer/electronic transfer requests.

10.4 Movement of Terrorist Fund

Extra care shall be taken while accepting the fund transferred from those countries which are vulnerable to terrorist activities and have low level of AML/CFT compliance. Bank shall regularly monitor the transaction in customer accounts such as charitable organization, nonprofit organization, trust, etc. which are highly vulnerable in terms of source of funds and uses of funds. Bank shall not accept the fund in case it has reasonable ground to believe that funds are transferred to assist the terrorist and money launderers.

11. Annual Turnover and Source of Fund

The effectiveness of on-going transaction monitoring and due diligence is largely depended on the customers' profile and source of funds. Source shall be disclosed on the transaction as per the regulatory threshold. If the Bank deems necessary to obtain sources from AML/CFT risk perspectives, source shall be taken even on the transaction lower than the regulatory threshold.

Banks shall obtain the information as source of funds of the customers at the time of establishing any business relationship or while conducting CDD. Customer declares the source of fund and expected annual turnover while opening accounts or establishing the relationship. Bank must deny collecting or accepting deposit if the source of fund is not disclosed or Bank is not convinced as reliable source disclosure.

12. Self-Assessment

Bank develops self-assessment system for monitoring and assessing the risk on AML/ CFT and KYC. Self assessment shall be conducted on half yearly basis within the standardized scope and format. The self assessment should advise management whether the internal procedures and statutory obligations of the Bank have been properly discharged. Risk Management Committee and AML Committee review the self assessment report and submit to Board for information and needful decisions.

13. Record Keeping and Retention

Documents and information related with identification and verification of customer and beneficial owner, documents and records related to domestic and foreign transaction with the client and or beneficial owner, records pertaining to account opening and the documents as specified by regulatory authorities shall be preserved for at least Five Years. Bank may keep such record in digital form in such a way that they can be retrieved as and when required to the best possible. The identification document and transaction data shall be provided to the competent authorities upon request.

14. PEPs, Sanctions and Watch List

Bank maintains a database of name, address and other available details of Politically Exposed Persons (PEPs), High Ranking Officials, Influential Persons and Persons/Institutions sanctioned by OFAC, UN, HMT, EU and / or as circulated by regulatory authority. Such data base shall be regularly updated and that database shall be screened while establishing relationship with the customers.

15. Media Monitoring and Adverse Media

Media monitoring will be supportive for the information of existing customer involvements on money laundering, financial fraud, drug trafficking, financial threat, organized crime, financial terrorism, bribery and corruption, human trafficking, tax evasion and more. Bank can use information from newspapers in print or online or broadcast news across radio and TV, blogs, web posts and other unstructured sources as a source of adverse media. Persons found on the news who are engaged on money laundering and financing on terrorism shall be screened on the Bank's customer data base whether they are Bank's customer or not. Customer having adverse media news and information shall also be recorded for customer identification purposes.

16. Training

All staff members of the Bank shall be adequately trained on the matter of AML/CFT and KYC. It is mandatory to all staff to sign and provide the self-declaration form regarding confirmation of reading and understanding of AML/CFT and KYC Policy, Procedures and Guidelines related with the AML/CFT and KYC. Bank shall retain the documentary evidencing the trainings and other program conducted with information of date of training, topics and staffs receiving the training.

Bank shall provide the training and awareness program to newly recruited staff within 6 month of their appointment and to its existing staffs at least on annual basis to keep them updated in AML/CFT and KYC.

Awareness program on AML/CFT and KYC Policy, Procedures and Guidelines along with requirement and responsibility shall be conducted for Senior Management and Board of Directors.

17. Customers and General Public Awareness

Bank conducts the customer awareness program on the matter of AML/CFT and KYC. Group of customers, shareholders and other relevant stakeholders shall be educated on the need, value and implications of AML compliances. Bank also initiates the social awareness program on the matter of money laundering and terrorist financing.

18. Independent Testing

Internal audit independently examine and assess the effectiveness of the AML/CFT and KYC implementation in the Bank. Internal Audit presents and submits the report on half yearly basis to Audit Committee, AML Committee and Risk Management Committee. Internal audit examine the compliance of AML/CFT and KYC in branches and departments in course of general audit plan. Statutory Audit also examines the effectiveness of AML/CFT and KYC compliance under its audit plan. Any deficiencies should be identified and reported to senior management together with a request for a response indicating corrective action taken or to be taken and a deadline.

19. Payable Through Account (PTA)

Payable-through accounts as correspondent accounts are used directly by third parties to transact business on their own behalf. Institution providing the correspondent banking services allows its correspondent banking clients' accounts to be accessed directly by the customers of that correspondent, e.g., the customers of the correspondent may have cheque writing privileges or otherwise be able to provide transaction instructions directly to the institution. Bank does not provide the payable thorough account facilities on any correspondent relationships.

20. Downstream Services

A downstream correspondent relationship occurs when a correspondent bank client provides correspondent services to other banks, domiciled inside or outside their country, to facilitate international products and services on behalf of the downstream correspondent's clients. Bank does not offer downstream correspondent services. Nested transactions are also not allowed.

21. Service of Third Party / Business Partners / Vendors

Bank shall review the AML/CFT and KYC compliance of third party / business partners / vendors before appointing them to provide banking service to Bank's customers or to Bank. Bank shall not establish any relationship with third party / business partners / vendors if bank believes that they are not adhered with country's policies in AML/CFT. The agreement between the Bank and third party / business partners / vendors shall contain the provision related to AML/CFT and such agreement shall be compulsorily reviewed by Chief/Head- AML Officer.

22. Formulation of Procedures, Guidelines and Manuals

Appropriate procedures, guidelines and manuals required for the effective implementation of the provision contained in this Policy will be prepared. The procedures, guidelines and manuals shall be constructed as the part of this Policy and shall be read in conjunction with the provisions contained in this policy. CEO is authorized to approve appropriate procedures, guidelines and manuals and same shall be furnished to the Board for information.

23. Miscellaneous

23.1 Confidentiality

Information collected from customers for the purpose of opening of account is to be treated as confidential and details thereof should not be revealed for any other purposes.

23.2 Safe Custody and Locker

Bank follows the identification procedures under normal KYC practices. Bank provides the facility only to the customer. Locker facility is graded as High Risk, Medium Risk and Low Risk based upon the risk assessment under AML/CFT.

23.3 Customer Service/Relationship Managers/Tellers/Foreign Exchange Dealers

Staff members who are dealing directly with the public are the first point of contact with potential money launderers so their roles are vital for fighting against money laundering. The front line shall be made aware of their legal and regulatory responsibilities. Bank's reporting system shall be made clear to the front line.

23.4 Simplified KYC

Bank may form the procedures for the simplified KYC for the customer having low social and financial status. There would be separate form for simplified KYC. Simplified KYC is applicable for the low risk customers.

23.5 Development and Review of Products and Services

All the products and service developments goes through the assessment from AML/CFT perspectives. AML Officer reviews the products and service development. Bank establish criteria of identifying and assessing ML/TF risks that may arise in relation to new products, services, business practices and delivery mechanisms including the review of existing products and services on on-going basis.

23.6 Prohibition of personal accounts for business purposes

Bank shall not allow personal accounts to be used for business purposes except small businesses and professions where the Bank is satisfied with KYC profile of the account holder, purpose of transactions and expected turnover of the account keeping in view financial status & nature of business of that customer.

24. Implementation and Review

This Policy will be effective upon the approval of BoD. It shall be reviewed annually. In case there is a conflict between the contents herein and laws, instructions and regulations issued by regulators or legislators, the stricter provisions shall be applied.

25. Repeal and Saving

This policy shall supersede the Bank's Know Your Customer and Anti Money Laundering / Combating Financing in Terrorism Policy 2016 and Customer Due Diligence Procedure (CDD Procedure) 2016 approved by the Management Committee Meeting No. 587 on November 28, 2016. Any acts done, actions taken under the Policy shall be deemed to have been done and taken under this Policy.