POLICY ON-
COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION

1st Policy- June 2014
Second Revision- November 2017
Third Revision- December 2018
Forth Revision- January 2020
Fifth Revision- June 2021
Sixth Revision- September 2022
Seventh Revision-August 2023
Eight Revision – May 2024

May 2024

HBL हिमालयन बैंक लिमिटेड Himalayan Bank Ltd.

(A class Financial Institutions Licensed by Nepal Rastra Bank Bank)

Table of Contents

1. ABBREVIATION (USED IN THIS POLICY)

ALPA	ASSETS (MONEY) LAUNDERING PREVENTION ACT
AML	ANTI MONEY LAUNDERING
APG	ASIA PACIFIC GROUP (OF MONEY LAUNDERING)
BCBS	BASEL COMMITTEE ON BANKING SUPERVISION
BOD	BOARD OF DIRECTORS
CAP	CUSTOMER ACCEPTANCE POLICY
CBS	CORE BANKING SYSTEM
CDD	CUSTOMER DUE DILIGENCE
CFT/CTF	COUNTERING TERRORIST FINANCING
CICD	COMPLIANCE AND INTERNAL CONTROL DEPARTMENT
CIP	CUSTOMER IDENTIFICATION PROCEDURE
CPF	COMBATING PROLIFERATION FINANCING
CO	COMPLIANCE OFFICER
CTMP	CUSTOMER TRANSACTION MONITORING PROCEDURES
DNPBP	DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS
ECDD	ENHANCED CUSTOMER DUE DILIGENCE
EDD	ENHANCED DUE DILIGENCE
EOO	EXECUTIVE OPERATING OFFICER
FATF	FINANCIAL ACTION TASK FORCE
FIU	FINANCIAL INTELLIGENCE UNIT
FP	FINANCING OF PROLIFERATION
HBL	HIMALAYAN BANK LIMITED
KYC	KNOW YOUR CUSTOMER
ML	MONEY LAUNDERING
NID	NATIONAL IDENTIFICATION DOCUMENT
NRB	NEPAL RASTRA BANK (CENTRAL BANK OF NEPAL)
PEP	POLITICALLY EXPOSED PERSON
PIP	PEOPLE IN INFLUENCING POSITION
PF	PROLIFERATION FINANCING
PTA	PAYABLE THROUGH ACCOUNTS
RM	RISK MANAGEMENT
STR	SUSPICIOUS TRANSACTION REPORT
TF	TERRORIST FINANCING
TTR	THRESHOLD TRANSACTION REPORT
TBML	TRADE BASED MONEY LAUNDERING
UBO	ULTIMATE BENEFICIAL OWNER

2. GENERAL PROVISIONS

This Policy represents the basic standards of Anti-Money Laundering and Combating Financing of Terrorism and Proliferation (hereinafter referred to as AML/CFT/CPF), Know your customer (hereinafter referred to as KYC) and Customer Due Diligence (hereinafter collectively referred to as CDD) procedures within Himalayan Bank Limited (hereinafter referred to as the Bank).

All relevant employees must be thoroughly familiar with and make use of the material contained in this Policy. Extract of this Policy shall be posted on the website of the Bank (www.himalayanbank.com). Full policy shall be posted in intranet site of the bank(hblonline.com) so that it shall be readily available to all relevant employees.

This Policy shall be renewed on annual basis in general. Updated versions shall be introduced and distributed to all concerned. Exception to this Policy must be approved by BOD or the entity authorized by the BOD. All exception must be documented with reason for the exceptions, including review date and where necessary, include an action plan and timetable for compliance with the Policy. The Policy shall become effective upon approval of renewal/amendment by the BOD.

This policy is applicable for Bank, its subsidiaries, Branches and all the employees.

This policy and procedures contain:

Part A: General Information and Definition
Part B: Bank's policies to combat ML/TF/PF
Part C: Miscellaneous
Part D: Duties and responsibilities
Part E: Annexure

3. PREAMBLE

Money Laundering (ML) is the processing of criminal proceeds to disguise their illegal origin. ML is a major concern, and it has been recognized as a major social problem and crime by the governments around the world. In response to the international community's growing concern about the problem, most global organizations and national governments have been actively pursuing programs against Money Laundering (ML), Terrorist Financing (TF) and Financing of Proliferation (FP).

To ensure that funds generated through illegal activities are not channeled within the financial system of a country irrespective of its origin. The Financial Action Task Force (FATF) established by countries of Group of Seven (G7) has come up with strong recommendations against criminal activities related to money laundering and Terrorist Financing. Since Nepal is a member of Asia Pacific Group on Anti-Money Laundering (APGML- a FATF-Style Regional Body) it is the duty of every financial institution of the country to check and control money laundering related activities. As these institutions' activities extend beyond the political boundaries of a country, it would be pertinent to devise/implement processes on anti-money laundering that are of international standard.

Nepal, in line under direction from FATF, has first promulgated act to address Money Laundering i.e. "Asset (Money) Laundering Prevention Act, 2008". The act mainly directs and prohibits Bank/ financial Institutions to collect deposit (fund) from customers that have been generated from illegal source.

Act clearly defines that Banks/ FI institutions should not be involved even in helping its customers to conceal, transform, transfer, hide its sources or misrepresent it. They should immediately inform details of such fund/transactions to the "Financial Information Unit (FIU)" at Nepal Rastra Bank (Central Bank of Nepal), a focus center that has been established under the Act and is the main concerned authority for controlling/monitoring deflection of currency or Money Laundering in Nepal.

HBL is committed to develop and implement appropriate policies and procedures to control AML/CFT/CPF and follow KYC policy guideline and update them on time-to-time basis in line with the changing environment both domestic & international front.

This policy document has been prepared in line with "Asset (Money) Laundering Prevention Act, Anti Money Laundering Prevention Rules and Directive issued by Nepal Rastra Bank (NRB) and Financial Intelligence Unit (FIU) from time to time.

However, if there is any changes made in the regulations, Act, Directive of Central Bank and Government regarding AML/CFT/KYC issues after implementation of this policy, they supersede this policy.

PART A: GENERAL INFORMATION AND DEFINITIONS

4. Information and Definitions:

4.1 **The Bank** means Himalayan Bank Ltd.

4.2 **The Board** means Board of Directors of Himalayan Bank Ltd.

4.3 **Chairman** means the Chairman of the Board of Directors of Himalayan Bank Ltd.

4.4 **AML/CFT Committee** is committee formed under the BOD to monitor/review the status of AML/CFT/KYC issues of the bank.

4.5 **AML/CFT Unit** is a unit established to look after the AML/CFT/KYC issues of Bank on full-fledged manner which is named as **'AML Unit'** in the organogram of the Bank.

4.6 **Chief Executive Officer (CEO)** means person/professional appointed as The Chief Executive of the Bank, appointed by the Board and entrusted with overall Management, Administration and Operations of the Bank and accountable to the Board.

4.7 **Competent Authority** is who acts in relation to the exercise of any power means the Board, Committee under Board, CEO, Head of Operations, Branch Managers, Department Heads or any other authority to whom such power is delegated by the Board or CEO from time to time.

4.8 **Compliance and Internal Control Department (CICD)** is the Department which looks after overall compliance and internal control of the bank.

4.9 **Customer:** The person or entity that maintains account or someone on whose behalf an account is maintained with the Bank or those on whose behalf an account is maintained i.e. owner is called customer. Any person or entity connected with a financial transaction that may impose significant reputational or other risks to the Bank is also considered as customer for the purpose of this document e.g. walk in customers requesting for one-off transaction.

4.10 **Walk in customer:** A customer who does not have account with us but avails services from the bank for himself or for others.

4.11 **Branch Managers** means heads of branches of the Bank.

4.12 **Dy Branch Managers** is Branch Manager who is 2nd head in the branch.

4.13 **Alternate Branch Manager**: Who works in absence of Branch Managers.

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

4.15 **Executive Operating Officer (EOO)** means the Officer or such designated official having other titles of the Bank, who shall be responsible for overall Operations of the Bank.

4.16 **Reporting Cell** is the department which collects, compiles, verify all the reports to be sent to Central bank and other concerned department.

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

4.18 **Legal Department** means the Department formed to ensure legal matter related to various laws and regulations on behalf of Banks.

4.19 **This Policy** refers to "Policy for Combating Money Laundering and the Financing of Terrorism and Proliferation.

4.20 **Act", "Rules" and "Directive"** refer to the Asset (Money) Laundering Prevention Act 2064 and Asset (Money) Laundering Prevention Rules 2073 and "Directive" will refer to the directive issued from Nepal Rastra Bank and Financial Information Unit.

4.21 **Legal Person (Entity)**: Any company, corporation, proprietorship, partnership firm, cooperatives, or any other body corporate, association, club, trust or individual that has legal standing in the eyes of law.

4.22 **Transaction**

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

1. *Establishing any kind of business relationship,*
2. *On boarding customer (account opening),*
3. *Any deposit or collection, withdrawal, exchange or transfer of funds in any currency or instruments, payment order by electronic or any other means,*
4. *Any payment made or received in respect of a lottery, bet or other game of chance,*
5. *Any payment made or received in satisfaction, in whole or in part, of any contractual or other legal obligation*
6. *Use of any type of safe deposit box (locker),*
7. *Entering/establishing into any fiduciary relationship,*
8. *Establishing or creating a legal person or legal arrangement, or*

9. Such other act as may be designated by the Government of Nepal by publishing a notice in the Nepal Gazette.

4.23 **Employee (Staff)** of the Bank as defined in the Staff Service Bylaws of the Bank.

4.24 **Politically Exposed Persons (PEP) and People in Influencing Position (PIP)- Domestic, Foreign and International**

Domestic High Profile Person/ Domestic Politically Exposed Persons (PEP)are any individual with a high profile political or bureaucratic role, or who has been entrusted with a prominent public function or as designated by the Govt. of Nepal upon the recommendation of National Coordination Committee.

Foreign PEPs/PIPs are individuals who are or have been entrusted with a prominent public functions by a foreign country, for example the Heads of State or of government etc.
International PEPs/PIPs are individuals who are high ranking officials in international Organizations like, UN, SAARC, ILO, etc.

As per this policy, Indicative list of Domestic High Profile Persons/Politically Exposed Persons or People in Influential Position have been as illustrated in **Annexure-1.**

4.25 **High Net worth Individual Customer:** Individual customer with average annual total deposit in the Bank exceeding NPR 50 Million or more is categorized under high net worth individual.

4.26 **Financial Action Task Force (FATF)**
Financial Action Task Force (FATF) is an inter-governmental body established in 1989. Its purpose is to develop and regulate national and international policies for combating money laundering and terrorist financing related activities. It also targets to bring legislative and regulatory reforms in these areas. It has published 40 Recommendations and 9 Special Recommendations in order to meet these objectives worldwide and continue to issue guideline to Bank FI globally and working closely with Central Bank/ Government to combat Money Laundering/ Terrorist Financing and financing of proliferation.

4.27 **Asia Pacific Group on Money Laundering (APGML)**
Asia/Pacific Group on Money Laundering (APGML) is an international organization consisting of 40 members and a number of international and regional observers including the United Nations, IMF and World Bank.
APG is closely affiliated with Financial Action Task Force (FATF). All APG members commit to implement the FATF's standards for anti-money laundering and combating financing of terrorism effectively.

4.28 **Basel Committee on Banking Supervision (BCBS)**
BCBS recommends sound KYC policies and procedures to support overall safety and soundness of banks and financial institutions and to protect integrity of financial systems by reducing chances of these institutions being used for money laundering, terrorist financing and other illegal activities.
In October 2001, the BCBS published a paper on "Customer Due Diligence for Banks", which was supplemented in February 2003 by the "General Guide to Account Opening and Customer Identification". This paper identifies four essential elements for a sound KYC program viz. Customer Acceptance Policy, Customer Identification, Ongoing Monitoring of higher-risk accounts and Risk Management.

4.29 **Financial Intelligence Unit (FIU)**
Financial Intelligence Unit (FIU – Nepal) is a national agency responsible for receiving, processing, analyzing and disseminating financial information and intelligence on suspected money laundering and terrorist financing activities to the relevant law enforcement/investigative agencies and foreign FIUs. It was established on 21 April, 2008 under the section 9 of the Assets (Money) Laundering Prevention Act, 2008 within the Nepal Rastra Bank (the central bank) as an independent unit.

4.30 **Money Laundering (ML)**
Money laundering is the process where the source of illegally obtained funds is channeled through a series of transfers and deals that can eventually obscure its original source and present it as legitimate income or

assets. The amount involved can be large at times. However, these can also be broken into small and collected ransoms in order to bury their originating source or use in criminal activities.

Usually, Money laundering has three stages. **i.e. Placement, Layering and Integration.** These stages may occur separately, simultaneously or in phases overlapping one other. In all the three stages the money obtained illegally are brought into the financial system through financial institutions.

4.30.1 Stages of Money Laundering

4.30.1.1 Placement

The physical disposal of cash proceeds derived from illegal activity could be done through:

1. *Depositing a large amount of cash in numerous small amounts (smurfing).*
2. *Hoarding of deposits in others name who has tax blanket*
3. *Setting up a cash business as a cover for banking large amount of money.*
4. *Investing in shares and other investment products*
5. *Mingling of illegal cash with deposits from legitimate business e.g. car and antiques dealers.*
6. *Hoarding of deposits in personal names instead of company to avoid applicable taxes*

4.30.1.2 Layering

Layering is the practice of separation of illegal money from its original source by creating complex layers of financial transactions designated to disguise the audit trail and provide anonymity. The purpose is to confuse the audit trail and break the link from the original crime. The examples are as follows:

i. *A Company passes money through its accounts under cover of bogus invoices, merely to generate additional transactions.*
ii. *A customer raises a loan on the security of a deposit (from illegal business) in another bank to help break the connection with illegal funds.*
iii. *A customer incurs large credit card debts from an account.*
iv. *Customer buying in cash and en cash against bank trail.*

4.30.1.3 Integration

If the layering process succeeds, integration schemes place the launched funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds. It is a scheme to move illegal money into the legitimate economy so that no one would suspect its origins.

4.31 Customer Due Diligence (CDD):

CDD is the process of identifying and evaluating the customers and the assessment of customers risk as part of KYC. Customer Due Diligence (CDD) is the key part of process wherein the bank conducts voluntary investigation to justify the underlying transactions purporting with necessary documents but not for any legal implication/ purpose.

4.32 Enhanced Customer Due Diligence (ECDD):

It refers to the additional due diligence pertaining to the identity of the customer, source of income, nature and value of transaction and others specified by NRB directives and as per AML CFT Manual.

4.33 Know Your Customer (KYC)

Know your customer (KYC) is a part of Customer Due Diligence that Banks must carry out to identify its customers and ascertain relevant information for carrying out financial transactions with them.

4.34 KYE – Know your Employee

KYE brings in sharp focus the need for thorough checks on employees' credentials and proper screening of candidates to prevent the hiring of undesirables.

4.35 Risk Categorization - High Risk /Low Risk/Medium Risk.

Based on analysis of different parameters like Geography, Products and Services, Delivery Channels etc. singly or jointly customers are categorized with High, Medium or Low Risk.
An indicative list of High Risk/low Risk and Medium Risk customers is given in **Annexure- 2** which shall be updated from time to time.

4.36 Shell Bank/Entity

"Shell Bank" means a bank which has no physical presence in the country in which it is incorporated, license or located, and which is not affiliated with a regulated financial service group that is subject to effective consolidated supervision.

A Shell Entity serves as a vehicle for business transactions without having any significant assets or operations of its own. Shell corporations in themselves may not be illegal as they may have legitimate business purposes. However, they can also be a main component of underground activities, especially those based in tax haven zone/country.

4.37 Terrorism and Proliferation Financing

Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organizations directly or indirectly as defined in the FATF Recommendations. Terrorism Financing involves the raising and processing of funds to supply terrorists group/organization with resources.

Proliferation Financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

4.38 Non-Resident Nepali (NRN) is a Nepali citizen that has migrated or permanently/temporarily residing in a foreign country in line with the provision of the prevailing Act or a person whose father, mother, grandfather or father-in-law were citizens of Nepal in the past and later acquired the citizenship of a country other than a member country of the South Asian Regional Cooperation (SAARC), holding foreign passport/citizenship is considered as non-resident Nepali.

4.39. KYC Compliance Officer(s) are designated staff of the Bank stationed at Head/Corporate Office and/or Branch to ensure day-to-day compliance of internal policies/procedures related to AML/CFT/KYC or CDD and or make ongoing evaluation of the efficacy of the policies and procedures. They should be the focal points for managing AML/KYC and CDD related matters.

4.40 Ultimate Beneficial Owner refers to the natural person(s) who ultimately owns or controls a customer and or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Reference to 'ultimately owns or controls' and 'ultimate effective control' refer to situations in which ownership/control is exercised through a chain of ownership (more than 10% directly or indirectly) or by means of control other than direct control.

Beneficial owner can be either declared or undeclared but exercises ultimate control over the account or the transaction.

Guardian in the case of minor account, mandatee in the case of mandated account, signatory of the account (including joint account), locker operator (in the case where locker holder and locker operator are two different persons) etc. are regarded as declared beneficial owner.

Undeclared beneficial owner is such an individual who cannot be seen in documents and records or does not own any shares or hold any formal ownership but ultimately exercises control (or ownership) over the account and transaction. So, it is difficult to trace and establish undeclared beneficial owner.

4.41 Fraud is an intentionally deceptive action designed to provide the perpetrator with an unlawful gain or to deny a right to a victim. Types of fraud include tax fraud, credit card fraud, wire fraud, securities fraud, and bankruptcy fraud.

4.42 Sanction Programs:

Sanction Program of a bank typically involves measures to ensure compliance with national and international sanctions. This includes screening customers and transactions against sanctions lists, implementing risk-based due diligence, and maintaining robust internal controls to prevent dealings with sanctioned individuals or entities. The goal is to prevent bank from regulatory fines/penalties and also reputational damage.

4.43 Risk Based Approach (RBA)

The approach of management which focuses on identifying and addressing potential risks of money laundering and terrorism financing. The core of this approach is to create the match between "risks and controls" by understanding of the ML/TF risks to which the banks are exposed and apply AML/CFT measures in a manner and to an extent which would ensure mitigation of these risks.

4.44 Threshold Transaction Report (TTR):

Threshold Transaction Report (TTR) is a report that Bank is required to file to FIU-Nepal for deposit, withdrawal, exchange of currency, or other payment or transfer; if it exceeds prescribed threshold limit. Following are the transaction limit currently set by the regulator to report to FIU-Nepal within Fifteen (15) days of transaction through goAML system.

i. *Single or multiple CASH deposits by a customer equal or above NPR One (1) million in a day.*
ii. *Single or multiple Cash withdrawal by a customer equal or above NPR One (1) million in a day.*
iii. *Single or multiple Cross border electronic or Wire Transfer by a customer equal or above NPR One (1) million in a day*
iv. *Single or multiple Exchange of Foreign currency by a customer equivalent to NPR Five (5) Hundred Thousand and above in a day.*

4.45 Suspicious Transaction:

A transaction, including an attempted transaction, whether or not made in cash, which to a person acting in good faith; Gives rise to a reasonable ground of suspicious that it may involve proceeds of an offenses specified in law and regulations, regardless of the value involve.

- *Seeks to conceal or disguise the nature or origin of funds derived from illegal activities*
- *Appears to have no economic rationale or bonafide purpose*
- *Appears to be in circumstances of unusual, or unjustified and complex in nature.*
- *Appears to be deviated from profile, character and financial status*
- *Seems to be made with the purpose of evading the legal and regulatory reporting requirements*
- *Found to be conducted to support the activities relating to terrorism*

4.46 Suspicious Activity: Any activity of the customer that gives rise to suspicion because such activity is unusual or that is not in accordance with bank's understanding about the customer based on customer due diligence

4.47 Suspicious Transaction/Activity Report:

A report to be made by the Bank to Financial Intelligence Unit (FIU) on any suspicious transactions or any attempts under the provisions of "Parichhed 3, 7dha- Asset (Money) laundering prevention Act 2064" and point no. **16** of NRB Directive no. 19.

4.48 Wire Transfer:

Any transaction carried out on behalf of an originator (both natural persons and legal entities) through the bank by electronic means with a view to making an amount of money available to a beneficiary person at another FI.

4.49 FATCA Reporting:

Bank shall comply with the provision of 'Foreign Accounts Tax Compliance Act' (FATCA) as per requirement of US Law and NRB Guidelines.

4.50 Family Member:

As per BAFIA, Family members are defined as Husband/wife, Son/Daughter In law/Daughter/Adopted son/Daughter, Father/Mother, Stepmother, Elder Brother/Sister-In-law taken care, Younger Brother In law and Sisters.

4.51 Egmont Group:

The Egmont Group of Financial Intelligence Units is a network of Financial Intelligence Units (FIUs) around the world. As a global organization, the Egmont Group facilitates and prompts the exchange of information, knowledge, and cooperation amongst member FIUs. The Egmont Group provides FIUs with a platform to securely exchange expertise and financial intelligence to combat money laundering, terrorist financing, and associated predicate crimes.

4.52 Modern Slavery and Human Trafficking (MSHT)

Modern slavery is a broad term that encompasses a number of unethical practices such as slavery or forced labor (including child labor), debt bondage, slavery like practices, servitude, deceptive recruiting, forced marriage, prostitution, organ trafficking and human trafficking.

Likewise, Human Trafficking is the use of violence, threats or coercion to transport, recruit or harbor people in order to exploit them for purposes such as forced prostitution, labor, criminality, marriage or organ removal.

4.53 Payable Through Account (PTA):

Payable Through Accounts means an account maintained at the correspondent bank by the respondent bank but which is accessible directly by a third party to effect transactions on its own behalf.

4.54 Conductor:

Conductor is a natural person who carries transaction on behalf of others or self. The information regarding natural person should be provide while TTR/STR/SAR reporting through goAML software. It plays vital role while tracking the suspect person.

Other than the terms specifically defined here-in- above, the terms used in various sections of this policy shall have the same meaning as has been defined under various other policy/documents of the Bank and the applicable laws of country and NRB Directive wherever relevant.

PART B: BANK'S POLICY TO COMBAT ML, TF AND PF

5. Objectives of the Policy:

The objective of this Policy and procedures is to prevent the Bank, employees and clients from being misused for money laundering, Terrorist Financing and Financing of Proliferation or other financial crimes by criminal elements. This Policy and procedures establish the general framework for the fight against money laundering and financing of terrorism and proliferation. The core objectives of this policy are-

i. *to prevent the bank mainly from being source/ platform to channel money earned through illegal means*
ii. *to protect from discredit - Bank should not have any kind of association, consciously or unintentionally, with criminals or facilitate them in handling proceeds of crime.*
iii. *to protect from the abuse of criminals - Involvement with them can expose the institution with the risk of being target of frauds.*
iv. *to build up good image so that the Bank attract customers whose source of wealth and funds can be reasonably established to be legitimate and do not pose an operational or reputation risk.*
v. *to comply with the "Asset (Money) Laundering Prevention Act" which forbids the act of accepting or allowing movement of funds that are not generated from a legal source.*
vi. *to comply with Directive issued by Nepal Rastra Bank (Central Bank of Nepal), other local laws and/or requirements of international Financial Institutions/Bodies,*
vii. *to protect its staff from unforeseen risks resulted to Money Laundering activities.*
viii. *to participate in the national and international drive against ML and FT/FP.*

6. Know Your Customer (KYC) Policy

Know Your Customer "KYC" policy is essential for the safety and ethical standards of the Bank's operations. The Bank understands that the availability of enough information of customer helps all other AML procedures and should be taken as essential element for effective management of ML risk. Keeping in view of specific requirement of NRB guideline, the bank has formulated KYC policy by incorporating the following key elements:

i. *Customer Identification Procedures (CIP)*
ii. *Customer Acceptance Policy (CAP)*
iii. *Customer Transaction Monitoring Procedures (CTMP), (on-going monitoring of accounts as per their risk grades)*
iv. *Risk Management (RM)*

7. Customer Identification Procedures (CIP)

Customer identification procedures involves undertaking customer due diligence (CDD) measures while commencing or continuing relationship with customer including identifying and verifying the customer and the beneficial owner on the basis of valid documents as prescribed in manuals/guidelines of the Bank which shall be in accordance with regulating laws and directives. It is essential to establish the true identity of the customers and be assured that the customers are not involved in any kind of money laundering and terrorist activities.

Under CDD, the Bank identifies and evaluates the customers and performs customer risk grading as part of know your customer (KYC) process, allowing banks to better identify, manage, and mitigate the AML (Anti-Money Laundering) related risks. The type and extent of customer due diligence shall depend on regulatory provisions, customer risk profile and other factors which shall be prescribed in manuals/guidelines of the Bank. Besides the risk perception, the nature of information/documents required for CDD also depends on the type of the customer and other attributes of the customer. The details of required documents for

different levels of CDD along with process of performing CDD and document verification shall be mentioned in manuals/guidelines of the Bank.

7.1 Natural person:

For the customer that is a natural person, the designated staff/ KYC Compliance Officer at the Branch should understand the intended nature of business and ensure that supporting identification documents as per NRB Directives, his / her residential address / location, recent photograph, other information and data are obtained and verified through independent and reliable source. Screening against sanctions/pep/pip of particular person (pseudo names, if any) to establish genuineness of the same is also carried out before establishing account relations

7.2 Legal Person (Entity):

For the customer that is a legal entity, the designated staff/ KYC Compliance Officer at the Branch should understand and verify its ownership and control structure including Ultimate Beneficial owners and ensure that supporting document as mentioned in NRB Directives are obtained and verified with originals. The Bank would deal only with the ones that are engaged in legitimate activity. The staff would establish to its satisfaction that it is dealing with a real or legally artificial person having proper identification and existence (natural or legal). The Bank should verify the identity of the person/s having authority to operate and control their account.

7.3 Customer Screening:

Customer screening for banking services involves a thorough process of assessing and verifying the identity of potential clients. This screening process typically includes: Identity verification, Sanctions Screening, PEP Screening, Blacklist Screening, AML Checks for Duplicate and NRB Blocked/Released Customer and KYC Documents. These screening processes are crucial for bank to comply with regulatory requirements, mitigate risks and maintain the integrity of our banking services. The details process for customer screening has been outlined in AML/ CFT/ KYC Manual.

7.4 Background/Information of customer:

Prior to establishing relationship with a customer, basic background information shall be obtained with regard to nature of the customer's business and sources of income, expected level of turnover/ transactions on the account and reasons for opening the account.

Prior to establishing relationship, screening is mandatory done against CIB blacklist, Multiple accounts, List of Account Blocked/Released by NRB and Law Enforcement Agencies and screening software to find out the background information of the customers

7.5 Customer Risk Grading (Risk categorization)

The Bank shall adopt customer risk grading as mentioned below –

a. *Low Risk*
b. *Medium Risk*
c. *High Risk*

Apart from these risk grading, Bank shall also categorize customers as PEP/PIP as per the indicative list illustrated in Annexure 1. For the purpose of Risk Assessment, PEP/PIP are considered as High Risk Customers.

All customers shall be assigned a specific risk grade. Illustrative list of customers under different risk category shall be as per **Annexure – 2** of this policy which shall be as per regulating Act, rules or directives in specific cases. A periodical review of the accounts should be conducted to re-assess the risk categorization.

The Bank shall obtain prior approval of Executive Operating Officer (EOO) or Senior Official designated by the EOO to establish or to continue business relation with PEP/PIP and High Risk customers.

Notwithstanding anything mentioned in the **Annexure – 2** of this policy,

i. the Bank may assign higher risk category to any customer if it deems necessary on the approval of EOO or Staff designated by the EOO

ii. the Bank may assign certain risk category to the customers using certain products and services of the Bank.

iii. The Bank may change risk category of such customers based on transaction or activity or risk profile information of the customer. Such change shall be from lower to higher risk category and vice versa.

7.6 Customer Due Diligence (CDD) Requirement

The Bank shall undertake customer due diligence measures, including identifying and verifying the identity of the customers and beneficial owners when,

i. *establishing business relationship,*
ii. *opening an account,*
iii. *carrying out occasional transactions above the threshold,*
iv. *carrying out fund transfer by electronic means,*
v. *suspicion about the veracity or adequacy of previously obtained customer identification information (customer's actual transactions/activities are not in line with information /documents provided by the customer during CDD or the Bank has a doubt about existing information/documents provided by the customer.)*
vi. *suspicion of money laundering or terrorist financing,*
vii. *performing transaction(s) anytime in relation to the high risk and politically exposed person,*
viii. *Conducting transaction with walk in customer*

7.7 Types of Customer Due Diligence (CDD)

Adopting the Risk Based Approach, The Bank classifies CDD under three types as mentioned below –

a. *Simplified Customer Due Diligence*
b. *Standard Customer Due Diligence*
c. *Enhanced Customer Due Diligence*

Types of information and documents to be collected from the customer and the process of performing due diligence under different types of CDD shall be as prescribed in manuals/guidelines of the Bank. Generally, Standard Customer Due Diligence should be carried out for all the customers and beneficial owners. In addition to Standard CDD, Enhanced Due Diligence shall be carried out for PEP/PIP, HNI and High Risk customers

7.7.1 Simplified Customer Due Diligence (Simplified CDD)

There are circumstances where the risk of money laundering or terrorist financing is lower or where adequate checks and controls exist elsewhere in national systems or where regulating laws and directives require to perform simplified CDD. In such circumstances, the Bank may apply Simplified CDD measures when identifying and verifying the identity of the customer and the beneficial owner. Subject to the compliance of Acts, laws and directives, the Bank may, on the approval of CEO, decide to perform Simplified CDD to a certain type of customers.

Simplified CDD shall not be carried out with respect to following customers or when following conditions exist: -

a. *If customer is foreigner.*
b. *If the customer is from country not fully compliant with international standards on AML/ CFT norms.*
c. *Foreign entity which is not licensed/regulated/supervised under the mechanism established to combat ML/TF/PF in consistent with the international standards.*
d. *Foreign individual/entity located in the territory which is not fully compliant with international standards on AML/ CFT norms as per FATF (Financial Action Task Force) or similar organization.*
e. *If customer is listed in stock exchange of high-risk countries not fully compliant AML/ CFT norms*
f. *If true beneficial owner/s is not clear.*
g. *If customers or true beneficial owner/s is PEP/PIP*
h. *Customers having annual transaction in the account more than NPR 1 Lakh.*
i. *If the customer is suspicious or doubtful.*

7.7.2 Standard Customer Due Diligence (Standard CDD)

The Bank shall perform Standard CDD for all types of customers subject to Simplified CDD for certain types of Low Risk customers. In addition to Standard CDD, Enhanced CDD is also applied for HR, HNI and PEP/PIP Customers.

7.7.3 Enhanced Customer Due Diligence (Enhanced CDD)

Enhanced CDD is conducted, In addition to Standard CDD, for High Net-worth Individuals, High Risk customers and PEP/PIP. It refers to the additional due diligence pertaining to the identity of the customer, source of income/wealth, nature and value of transaction and other information and documents as specified in the regulating Acts, rules and directives.

Bank shall follow appropriate measures of Enhanced CDD when establishing business relationship or conducting transaction with/of following customer:

(a) *Customer identified as high risk*
(b) Customer who conducts complex, unusual large transactions and unusual patterns of transactions or which have no apparent economic or visible lawful purpose,
(c) Transaction with customer of a country, which is internationally identified as inefficient or non-compliant country of international AML/CFT standards,
(d) PEP, his family member and person associated with PEP,
(e) High Net-worth Individual customers
(f) Customer suspected of ML, TF or other offense,
(g) Other customers as prescribed by the Regulator
(h) Transactions done through electronic medium which is systematical unusual and suspicious in nature

7.8 Physically present and Non-Face to Face Customers

The customer or their designated agent must be physically present at the Bank and have face to face contact/meeting with the designated staff or KYC Compliance Officer at the Branch. It is the responsibility of the KYC Compliance Officer of Branch to ensure that such contact or meeting is held. The original identification document must be verified during the same process.

The Bank may establish business relationship with Non-Face to Face customers via online or through other medium, which shall be done with a clear procedural guideline ensuring appropriate measures to protect the Bank from being used as a medium for money laundering or financing of terrorism. However, Account debit is not permitted in such accounts till all the documents are verified and customer is physically present.

Face to face meeting with concerned staff and Representative Officer deputed abroad is considered as physically present in the Bank. Meeting through Video conference or any other digital media where the identification of the customer can be verified, shall also be considered as Face-to-Face Meeting unless restricted by NRB.

7.9 Mandate:

In case of the account is to be operated by mandate (Power of Attorney), entire CIP and verification of residential address shall be applied to the customer and person authorized to operate the account. Thumb print and full KYC of Mandatee is compulsory.

Name, address, relationship and identification document and photograph of the guardian must be obtained along with the child's Birth Certificate for opening account of a “Minor”. Similarly, full KYC of locker operator need to be obtained if he/she is different from locker holder.

7.10 KYC (CDD) Review interval:

The Bank shall perform periodic CDD in the following time intervals -

- **Every year** in case of High Risk, PEP/PIP and HNI customers
- In **every 6 Years** in case of Medium Risk Customers
- **On need basis** in case of Low Risk Customers

Notwithstanding anything contained above, the Bank shall perform CDD review of customers immediately or in need basis-

- *If bank is suspicious about the true facts of KYC provided by the customers, immediately.*

- *If Bank comes to know any serious adverse news about the customer- on need basis*
- *If the customer's transaction/activity largely varies with existing CDD- immediately*

7.11 Collection of Thumb Print of customers:

While opening account of customers as per Section 4 (4) of AML Rules, Thumb Print of Account Operators shall be obtained on risk basis **on AOF/KYC Document or through Electronic Device (Bio-Metric).**

7.12 KYC of Walk-in customers:

As per Section 3 of the AML Rules, walking customer who carry out transactions like FCY exchange, Remittance, Deposit of NPR 0.1M (one lac) or above, identification of such customers with contact details shall be obtained **as per AML** CFT KYC Procedural Manual.

7.13 Exceptions to customer identification:

Any exceptions to customer identification procedures or cases not explicitly provided for would be approved by the Branch Manager or Department Head with the consent of the Designated KYC Compliance Officer of the Branch under intimation to EOO at Head Office. Reason/s of such exception must be documented.

7.14 Specific Identification Issues:

7.14.1 **Trust, Nominee and Fiduciary accounts**

Trust, nominee and fiduciary accounts can be used to circumvent customer identification procedures. While extra layer of security to protect the confidentiality of legitimate private banking customers, it is essential that the true relationship is understood. The Bank should be vigilant on whether the customer is using the name of another customer or person acting as a "front" or acting "on behalf" of another person as a trustee, nominee or other intermediary of the said person. If so, the Bank may require necessary precondition to be fulfilled i.e. a satisfactory evidence of the identity of any intermediaries, and of the persons on whose behalf they are acting, as well as details of the nature of the trust, or other arrangements should be sighted / established / held. Specifically, the identification of a trust should include the trustees, settlers/grantors and beneficiaries.

7.15 Identification of Customer's beneficial owner:

Identifying beneficial ownership is important in order to remove concealment and identify the actual individual behind the transactions and account activities. Bank shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner before establishing business relationship or conducting transaction with any customer.

For the purpose of identifying and updating Beneficial Owners in this line for new and existing customers, the reasonable measures can be, asking the customer to provide supporting official documents that justify beneficial owner, conduct open-source search, consulting commercial available information, account transaction /source monitoring, customer activity/behavior monitoring, information through normal course of the business/transaction etc. Further, if beneficial owner cannot be identified via any source, the Bank shall not perform any transaction with such customer.

7.15.1 Identification of Ultimate B/O of Entity Customers

The Bank should be vigilant in preventing corporate entities from being used by natural persons as a method of operating anonymous accounts. The Designated staff in the Branch, in conjunction with the respective Branch Manager / Relationship Manager should obtain information to understand the structure of the company, determine the source of funds and identify the ultimate beneficial owners and those who have control over the funds.

To establish the beneficial ownership of Entity Customers, The Bank shall take following elements in consideration. Any natural person, who satisfies any one or all the three elements as mentioned below, is a beneficial owner.

1. *Who owns more than 10% shares (directly or indirectly) of the customer (Entity)*
2. *Who has effective control of the customer*
3. *The person on whose behalf transaction is conducted*

Bank need to ensure and collect all the information that describes the ownership, control and structure of the entity, detail information of all the directors, account operators, signatories of the organization.

7.15.2 Identification of B/O of Individual Customers

Account Operators (Mandatee, guardians etc..) are considered Beneficial owners of Individual Customers. Bank need to ensure and collect all the Information and CDD documents of mandatee, parents/guardians in case of minor account, locker operator if he/she is different from locker holder etc. to identify the real beneficial owners of the account/transaction.

7.16 Politically Exposed Persons (PEP) and People in Influencing Position (PIP):

PEP/PIP means those persons as defined in regulating Act, Rules or Directives. The Bank shall gather sufficient information from a new customer, verify with the updated available list of PEP/PIPs to identify whether the customer is PEP/PIP or not. Following process should be followed while identifying the PEP/PIP:

a. Obtain information from customer (declaration from customer)
b. Obtain information from news media.
c. Judge and keep tab of the news of social media.
d. Obtain information from Commercial Data base

After evaluating as per above, Bank shall adopt the following additional measures if the customer or beneficial owner is either a **domestic**/foreign **or international** PEP:

a. Obtain approval from EOO or Senior Official designated by EOO at central level while establishing new business relationship and to continue business relation with an existing PEP/PIP.
b. To take all reasonable measures to identify the source of amount, fund and property of such customer or beneficial owner
c. Conduct ongoing monitoring of such customer and the business relationship
d. Apply Enhanced CDD measures

All types of PEP/PIP are considered as high risk customers and also they are considered PEP/PIP for **5 years** from the date of their retirement from their positions.

7.17 Negative news alert/Global/ Watch List Matches:

The Bank shall check, and screen own negative news alert cases through newspaper/media and other social media on continuous basis. Name Screening Software also provides Global Watch-List matches/sanctions lists which includes negative news as well. Further, the Bank shall check to ensure non-inclusion of individual/entity prior to establish any kind of relationship with the bank and then on periodic basis.

7.18 Correspondent Banking relationship:

Prior to establishing relation with correspondent bank, the Bank shall gather sufficient information about their correspondent Banks or Financial Institutions to fully understand the nature of their business and activities. The Bank shall carry out due diligence measures on establishment of every cross-border correspondent banking relationship by benching information received from third parties and or information available in public domain. Factors to be considered should include information on its ownership & management structure, major business activities, and location of business, money laundering prevention and detecting efforts, purpose of the account/ relationship, proper identification and CDD of third party using the correspondent banking. The CDD review for Correspondent Banks/FIs/Vostro partners will be as per the Wolfsberg Group Financial Crime Compliance Questionnaire (FCCQ) or Correspondent Banking Due Diligence Questionnaire (CBDDQ)

7.19 Super Agent/Principal Agent and Sub-agent:

The Bank shall obtain sufficient information from its Super/Principal agent and the CDD review for such agents will be done on annual basis in general as annexed in AML/CFT/KYC Procedural Manual. The Bank shall conduct CDD of Sub-agent on need basis through its Super/Principal agent to gather sufficient information as annexed in AML/CFT/KYC Procedural Manual. Moreover, Super/Principal Agents shall provide required CDD information/data of its sub-agents and customers as and when required by the Bank.

7.20 Refusal of Account Opening Request:

The Bank shall not open an account of a customer or maintain business relationship or transaction who cannot provide necessary documents, details and information for customer identification and verification as per CDD requirement, or the identification and confirmation of the customer cannot be made based on the documents, details and information provided in KYC details. If any such customer exists, the Bank shall terminate the business relationship with such customer and if necessary, shall notify the same information to FIU-Nepal. The Bank can refuse for account opening if the customer is not disclosing there as on for opening account, transaction volume etc.

The decision of refusal shall be properly documented. The basis of refusal of the account opening request shall be informed to the Compliance Officer at Head Office and the information of such refusal shall also be reported to CICD and circulated to all the Branches for their reference not to entertain those customers refused by one Branch.

7.21 Acceptable Identification Documents:

The Bank shall obtain copy of identification and other required documents of customers as prescribed by NRB Directives. Minimum document/certificate as specified by Central Bank of Nepal (NRB) from time to time must be obtained in all the cases. The details of Acceptable Identification Document shall be as per prescribed in latest Directives of NRB.

7.22 Identification and Verification by Third Party:

The bank may rely on a third party in undertaking some elements of customer identification and verification if the bank is satisfied that identification and verification of customer is carried out as per the guideline of FIU / international AML/CFT standards. No identification and verification of a customer made by third party shall be acceptable for the Bank if such third party or institution belongs to a country identified as a deficient country in compliance to the international AML/CFT standards or if such third party or institutions are not under regulation, control and supervision to prevent and combat money laundering and terrorism financing.

8. Customer Acceptance Policy (CAP):

The Bank shall not accept any individual/entity as its customer if the customer and beneficial owner of the customer cannot be identified / verified.

In case of business relationship with existing customers, where the Bank is unable to apply appropriate CDD measures due to unavailability of information and/or non-cooperation on the part of the customer in supplying the related information or documents within a reasonable time when demanded, the Bank may consider actions up to discontinuation/close of business relationship with such customers. The bank may even report suspicious transaction/activity report to FIU in case of suspicion and as required by the Bank.

The Bank Customer Acceptance Policy (CAP) lays down the following explicit criteria for accepting customers:

i. *Account shall be opened only in the natural or legal person's name. The name should be exactly the same that has been registered with government/government approved entities and consistent with the one appearing in the identification document. No account should be opened in anonymous or fictitious/blank name(s) or with confidential account number*
ii. *In case of Indian Nationals, If registration certificate issued by Indian Embassy doesn't contain full name but full name appears in any other documents, then the account shall be opened in full name.*
iii. *In case of character limit in CBS for long name as per legal documents, popular abbreviation can also be used as Account Name.*
iv. *Minimum information and documents must be obtained from the customer for opening account which must be valid and sufficient for customer screening and risk profiling.*
v. *No account shall be opened by an intermediary for third person.*
vi. *No account shall be opened without face-to-face contact with the customers. However, the account opened by Representative/Market Representative of the Bank shall be treated as the account opened by the staff itself. Customers having face to face contact/approach with Representative Officer of the Bank can be considered as self-present.*
vii. *No account (except Social Security/Online account) to be opened without complete KYC and if KYC of existing account cannot be updated, post restriction (Post No Debit) to be marked wherever applicable.*

viii. *If any person (individual or entity) is earlier inquired by law enforcement authority in connection with blocking the account (post no debit or credit or both) when such person was not the customer of the Bank and later if such person approaches the Bank for establishing business relationship and the Bank comes to know (based on available database maintained by the Bank) that the accounts of the person (in other BFIs) were once blocked by law enforcement authority, relationship with such persons will be established provided that the KYC Compliance officers ensures that the customer is no longer in account block list or where it could not be confirmed through the Bank's database, such customer will be asked to provide clearance letter from law enforcement authority. Where customer is unable to provide the clearance letter, account can be opened on the basis of declaration of the customer that he/she/it is no longer in account block status.*

8.1 Prohibited customers and transactions:

Bank shall prohibit following customers and transactions÷

1. *Who/which establish or maintain anonymous accounts, or accounts in fictitious names or transact in such accounts or cause to do so*
2. *Shell Banks*
3. *Who/which Maintain relationship with shell Banks or other entities which deals with shell banks*
4. *Who/which Establish an account or continue business relationship or conduct transaction with the customer who cannot provide documents, information and details required for the customer identification and verification as required by law and regulation.*
5. *Customers who provide conflicting Documents, information and details.*
6. *Individuals/Entities sanctioned by major sanction authorities such as United Nations, Office of Foreign Assets Control- United States, Her Majesty's Treasury-United Kingdom, EU etc.*
7. *Payment orders with an inaccurate representation of the person placing the order*
8. *Acceptance of payment remittances from other banks without indication of the name or account number of the beneficiary.*
9. *Payable through Accounts*
10. *Companies issuing bearer shares*
11. *Natural and legal person involved in producing and distributing illegal Arms and Ammunition*

8.2 Opening Accounts and Required Documents:

The decision to open an account for a new customer creates a legal relation between the customer and the Bank. Account opening decision is the prime responsibility of the Bank's department/branch heads. Strict examination relating to the prospective customer's identity must be executed prior to opening any new account and processing a transaction. The document requirement is as per the CDD requirement based on risk profile of the customer and as outlined in NRB Directives.

8.3 Certification of Documents:

The Bank shall verify the documents submitted by customers with the original at the time of account opening and executing banking transactions. The designated staff should verify their copies against the original documents and affix his/her signature as confirmation of such verification.

8.4 Re-submission Policy/Rejections Policy:

If the rejection of any customer or transaction is due to administrative errors or other minor non-compliance issues like incomplete documents, error in documents etc., customers shall have the option of re-submission in the Bank for different services such as Account Opening, Loan application, or Credit Card requests. However in cases where a transaction or customer is rejected due to regulatory concerns or on the ground of AML/CFT/KYC issues, then customer shall not be allowed for re-submission. List of such rejected customers/transactions shall be recorded, and STR/SAR are raised if required.

9. Ongoing Monitoring:

Ongoing due diligence is an essential element of effective CDD that should be carried out by the bank for ongoing monitoring in relation to the customer, beneficial owner or business. The Bank shall exercise ongoing due diligence of customers by carrying out the following activities

(a) Closely examine the transactions of customers in order to ensure that such transaction is consistent with the information of customer, the customer's business and risk profile thereon.

(b) Request for or examine the source of funds if it is necessary.
(c) Review and update the document, data, details or information of customers
(d) Regularly monitor cross border correspondent banking and wire transfer transactions and such customer relations.
(e) To perform other functions as prescribed by the Regulatory body and the Bank as deemed necessary from time to time.

9.1 Customer Transaction Monitoring Procedure:

The Bank shall have a robust automated transaction monitoring system to ensure that the accounts or transactions do have a valid purpose and are not used in Money Laundering and Terrorist Financing activities. Such system will support in identification of suspicious transactions relating to all the areas. The Bank shall develop comprehensive scenarios to detect suspicious transactions from the system. The extent of monitoring of accounts and transactions shall be guided by the degree of risk associated with the customer/transactions and the anomaly in the transactions with respect to the information disclosed by the customers. Concerned Branch Managers and AML/CFT Unit of the Bank will look after and analyze the alerts/reports generated by transaction monitoring system and perform appropriate reporting. Customer transaction shall be monitored automatically or manually whichever is feasible for the bank.

9.2 Customer's Risk Profile:

As a part of on-going monitoring **of existing Customers**, Risk category shall be assigned to the customers based on following parameters singly or jointly.
Based on Account turnover/transactions
Based on Occupation
Based on Nature of business/Activities
Based on Volume of Transactions.
Based on Products
Based on Geographical locations: 1. Domestic 2. International

9.3 Monitoring of Graded Accounts:

Account monitoring involves tracking transactions for unusual patterns or large amounts that may indicate illicit. It is a crucial measure to ensure regulatory compliance and prevent financial crimes.
The Bank shall be vigilant in case of frequent or large value movements of funds in any account irrespective of its category.

10. Recognition and Reporting of STR/SAR to FIU

The Bank shall provide suspicious transaction and activity of customer to FIU-Nepal through goAML system as soon as possible within three working days after detection from the initial suspicion if the following conditions exist in relation to the client, business or source of fund.

- If any transaction/activity is suspected or has reasonable grounds to be suspected of being related to money laundering and terrorist activity.
- If any transaction/activity is related to, or linked to terrorist activities, terrorist persons or terrorist organizations, or if there is evidence that may be used in such an act or by such person or organization, or if there is a reasonable basis for investigation.

The Bank shall give the report related to the suspicious transaction even if the client only attempts to do any transaction. The basis for identifying suspicious transactions, format, methodology and procedures for reporting suspicious transactions/activity shall be as per FIU Guidelines, Directives and Red flag indicators used by the bank. Some of the examples of the suspicious transactions/Activities are enlisted in **ANNEXURE-3.**

10.1 STR/SAR Decision Making Process

Transaction Analyst shall analyze in detail about the transactions and if found unusual then inform to STR reporting officer for further investigation who will investigate in detail from different angle to raise STR/SAR. STR Reporting officer and Head of AML CFT Unit shall discuss and take final decision whether to raise STR/SAR or not.

10.2 Threshold Transaction Report (TTR):

The Bank shall report Threshold Transactions Report through goAML system as per instruction outlined in NRB Directives, TTR Guideline and goAML Operational Guidelines.

11. Sanction Policy:

The Bank is firmly committed to complying with national and international economic sanctions by adhering to all relevant laws and regulations related to sanctions imposed by government authorities. The major component of sanction policy includes the processes for screening customers, transactions and counter parties against sanctions lists to identify and prevent dealings with sanctioned entities or individuals.

Sanction screening shall be the integral part of due diligence process and thus the sanction screening shall be conducted while updating identity, and conducing further due diligence. The Bank shall not establish any kind of relationship (customer, employee, vendor, consultant, service provider, business partner, etc.) with sanctioned individuals/entities listed in the Sanction List published by UN, OFAC, HMT-UK, EU. The Bank shall set up mechanisms for periodic review and update of the sanctions policy to align with the changes in law and regulations.

Sanction screening shall be done in an ongoing basis on prescribed period. Screening shall be conducted whenever there are any material changes in the legal entity like change in BOD members, change in shareholding pattern, change in management team, change in signatory etc.

11.1 Special provision on freezing of Account:

The Bank shall immediately and without delay block the account of specially designated persons, groups and organizations **involved in the terrorism/terrorist activities or** person, group or organization engaged or financing in the proliferation of weapons of mass destruction. The accounts belonging to or wholly or jointly, directly or indirectly, owned or possessed or held or controlled by and whose UBO is such person, group or organization, the Bank shall put full restrictions of accounts and the properties mortgaged/held in the bank. The bank shall report the details of such blocked account/property to concerned authorities for further action.

12. Risk Management (RM)

The Bank shall adopt risk-based approach in managing its ML/FT/FP risks and assess potential ML/FT/FP risks and implement measures and controls commensurate with the identified risk. The bank shall strengthen, make priorities and perform its activities to manage higher risks first and ensure that greatest risks receive the higher attention. Identification and assess of the money laundering and terrorist financing risks in accordance with its business and profession, scope, products, services or transactions of customers allows us to determine and implement proportionate measures and controls to mitigate these risks.

12.1 Risk Management through Three Lines of defense:

For the effective assessment, understanding, management and mitigation of ML/FT/FP risks, bank shall adopt three lines of defense. Identification and analysis of ML/FT/FP risks and effective implementation of policies and procedures to encounter the identified risk is the features of effective and sound risk management. The line of defense shall act as safeguard of the bank during the adversities and shall be liable for effective risk management.

a. First line of defense:

The first line of defense is provided by the front-line staff/Business Units and Operation Units to prevent ML/TF/PF risks. Business Units shall promote AML/CFT principles while doing business and manage the ML/TF/PF risks arising from the business. Business Units are responsible and liable for ongoing management of ML/TF/PF risks. The process of identifying, assessing and reporting AML/CFT risk events shall be done by front line staffs. Further, front line staff involved in business functions must ensure that appropriate controls are in place and operating effectively. Business units shall make an appropriate risk assessment before introducing any product or service and implement required mitigation. It shall be the responsibility of Second line of defense to assist business units/departments in this process.

b. Second line of defense:

The second line of defense is provided by related Control Departments in Head office, viz. Central Operations, Risk Management Departments, Compliance and Internal Control Department, AML CFT Unit to prevent ML/TF/PF risks in the bank.

c. Third line of defense

The third line of defense is provided by the internal audit. The internal audit shall review the activities of the first two lines of defense with the purpose to ensure that legislation, regulations and internal policies are processed effectively.

12.2 Risk categorization review interval:

Based on transactions and affiliation/engagement of the customers, account risk categorization to be reviewed at the time of KYC review or conducting periodic CDD/EDD.

12.3 Risk Assessment:

The Bank shall identify and assess the institutional risks on ML and TF and FP in accordance with its business or profession, scope, customer, products or services, geography, sectors, transactions or delivery channel etc. While assessing the risk, banks shall analyze and evaluate the risk related to AML/CFT based on the following topics and grounds:

***A**. Findings on National and Regional Risk Assessment report.*

***B**. Based on report/ data base of AML/CFT of international organizations.*

***C**. Commercial relations, threshold transactions and different natures of business, location, transactions etc.*

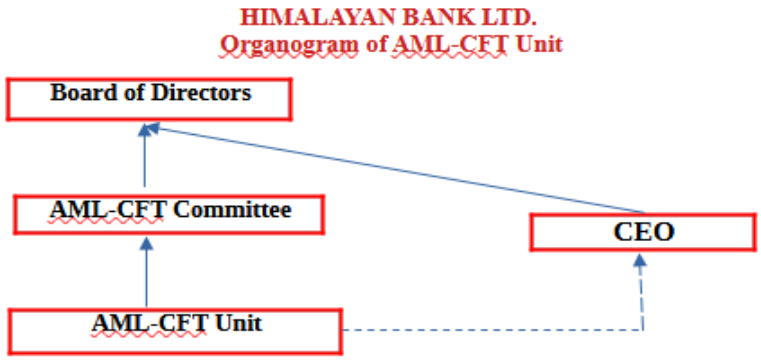
AML CFT Risk Assessment is done periodically covering the Sanction and ABC Risk Assessment and in accordance with ML/TF Risk Assessment Guidelines for BFIs issued by NRB and necessary update on the policy and procedural manual shall be done accordingly. A copy of Annual Risk Assessment report shall be sent to NRB and FIU-Nepal as per Regulatory instruction.

13. Internal Control:

BOD shall formulate and ensure implementation of necessary internal policies, procedure or controlling systems to comply with AML Act, Regulations and AML Directives from Central Bank.

Bank shall establish a separate AML/CFT UNIT with sufficient staffs and skilled resources headed by a managerial level AML Compliance Officer to comply the obligation pursuant to the provision of under preview of AML Act 2008 and the work, duties and rights of the AML Compliance Officer is as outlined in AML Act and as specified in **TOR of** NRB Directives.

The organogram of AML-CFT Unit is as follows:



AML CFT Committee under the BOD shall look after AML/CFT issues as directed/instructed by Central Bank and submits AML CFT status report on quarterly basis to the Board with necessary recommendations on procedures, development and give their review and observation and make appropriate decisions.

14. Wire /Electronic transfers (Domestic and Cross Border):

The Bank shall comply with the provision of Wire Transfers in accordance with Act, Rules and NRB Directives. The Bank's obligation is to correctly identify and confirm the customer by getting detail information as mentioned below for any wire transfer irrespective of currency or amount as per prevailing law.

The Bank should verify the correctness of full information received on electronic transfer such as name of the Originator and Receiver, Account number of Originator or Remittance Control Number (if does not process bank account number) and the ID number or address of the Originator and the Receiver. The full information of the originator and receiver required in general for outward wire transfer are as follows:

a. *Name of the Originator,*
b. *Account number of the originator or in the absence of it, a unique reference number,*
c. *Originator's address or, in the absence of the address, the citizenship or national identity number or customer identification number or date and place of birth, contact no, source of funds etc.*
d. *Name of beneficiary and account number or in the absence of an account number, a unique reference number, contact details, address etc.*
e. *Other information or details as prescribed by Regulator and/or as prescribed in fund transfer manual of the Bank*
f. *Purpose of transfer is to be mentioned properly/ clearly.*
g. *In International Electronic Remittance Transfer (including group transfer) the ordering bank or financial Institution, except in specified condition, shall send all the details of the originator and the payment order to execute the payment.*
h. *In Domestic Electronic Transfer, if any, the ordering bank/ FI shall include full information of the Originator and Receiver to process the payment as mentioned in above.*
i. *The Bank shall not implement the payment instruction without the full information of originator and receiver. If Payment instruction received without full information of originator and receiver, Remittance processing unit shall demand missing information from the ordering institution.*
j. *Unscheduled group transaction that increases risk of money laundering and terrorist funding should not be allowed.*

Bank, prior to initiating Wire Transfer, has to run down data filtration process to check if individual/ entities involves in transfer/ recipients are subject to sanctioned list. Wire transfers that does not match with the profile and nature of business shall be informed/reported to FIU. The Bank may reject or suspend any wire transfer with incomplete CDD or lacking required information on originator, beneficiary, source and intended purpose of wire transfer and or if the same is deemed suspicious in nature.

15. Terrorism Financing

Terrorism financing means providing financial support to any form of terrorism for terrorist activity including criminal activities from individuals or Entities. The Bank shall follow the instruction to comply with the provision for Terrorism financing in accordance with Act, Rules and Central Bank Directive. The Bank's obligation is to update about the information from the best possible means or mechanism regarding terrorist individuals, groups or organizations published by national and international organization. The list of persons involved in terrorist activities, groups or organizations shall be verified regularly if it is bank's customer/account holder and shall act according to the order if any matches observed with the published list.

The Bank shall develop necessary system to maintain updated designated lists in electronic form and shall conduct screening process on regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts with them.

15.1 Freezing of Financial Assets:

a. Nepal Rastra Bank may request the Bank to freeze the accounts or assets held by or for the benefit of the designated individuals/entities. If such request is received from NRB, the Compliance Officer at CICD shall send freeze order to Central Operations requesting them to freeze such accounts immediately.
b. The freeze order as aforesaid shall take place without prior notice to the designated individuals/entities.

16. Proliferation Financing:

Proliferation financing is defined by the FATF as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Preventing the proliferation financing is an important part of combating proliferation. The bank will adopt the measures outlined in AML rules and regulatory instruction on financing such party/ies and to disrupt the financial flows available to proliferators and to obstruct and complicate the procurement of the illicit goods, services and technology needed for the development of weapons of mass destruction and their means of delivery wherever applicable. The bank will process the freezing the assets if found any activities as Proliferation financing outlined above in compliance with FATF recommendations.

17. Trade based Money Laundering:

Trade-Based Money Laundering (TBML) involves the exploitation of trade to legitimize illicit funds. The Bank have policy in place to combat TBML, including CDD procedures, monitoring trade finance activities for suspicious patterns. Proper customer screening is done at the time of Trade finance related facilities as well as at the time of sending the payment against Sanctioned list of applicants as well as beneficiary.

Document to be checked whether the shipment is from sanctioned countries or whether the vessel is used from sanctioned entity or sanctioned countries using vessel tracking system in need basis and reject the proposal if the shipment is from or to sanctioned countries. Bank shall closely monitor transactions and business pattern to identify possible TBML.

18. Money Laundering in Credit:

Money laundering in credit facilities can occur when individuals or entities use borrowed funds to conceal the origins of illicit proceeds. The use of funds taken as loan can also be misused for money laundering purpose. This could involve taking out loans or credit lines using illegally obtained money and then repaying the debt using legitimate funds, thereby legitimizing the illicit proceeds. To combat this, the Bank shall implement strict CDD procedures to verify the source of funds for credit facilities, monitor transaction patterns for suspicious activities, and conduct ongoing monitoring of borrower activities to detect any unusual or suspicious behavior.

To analyze the inherent AML CFT Risk in proposed credit facilities to the customers, The Bank shall conduct a brief AML CFT Risk Assessment at the time of credit appraisal.

Loan of PEP/PIP to be approved by Senior Management (Province Head or above) even if it is within authority of concerned Branch Manager/In charge.

The Bank shall monitor the intended use of credit facilities by the customer and if any deviation is noticed on the intended use of loan and the nature of transactions, the bank shall report to FIU-Nepal for any STR/SAR.

19. Introduction of New Technology/Products

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 shall ensure that appropriate AML CFT Risk Assessment is done prior to introduction/execution of new technology and new products.

20. Fraud Detection:

a. *Fraud encompasses an array of irregularities and illegal acts characterized by intentional deception. It is usually taken to involve theft – the removal of cash and assets to which the fraudster is not entitled – or false accounting- falsification or alteration of accounting records or other documents. Improper and unlawful enrichment, improper use of assets and other items,*

and other fiscal irregularities. A business or organization may be exposed to various nature of frauds like external, internal, coercion, collusion.

b. *Common categories of fraud like balance sheet frauds, employees' frauds, suppliers' frauds, customer frauds, computer frauds, information technology frauds etc.*

c. Identifying fraud:

The Bank expects all its Directors, Alternate Directors, President, Officers, employees, consultants, contractors, counterparts and customers to observe the highest standards of ethics and to have a responsibility for fraud prevention and detection. Fraud prevention and detection matters shall be included in the Bank's induction programs and continuous career training.

d. Fraud reporting and investigation.

It is the responsibility of all staff to stay alert for occurrences of fraud or corruption and to be aware that unusual events, transactions or behaviors could be indications of actual or attempted fraud, corruption or money laundering.

21. Complete Record Keeping

The Bank shall preserve following documents, information and records accurately and securely for minimum **5** (**Five) years** after the termination of business relationship or from the date of transaction occurred with the customer.

a) *All documents and other information related to the identification and verification of customer and beneficial owner.*
b) *Customer's transaction related documents*
c) *Documents and details of account and business relation*
d) *All documents and records relating to domestic and cross border transactions*
e) *Suspicious transaction/activity reports of customers.*
f) *Records of Staff training including the attendees and subject material.*
g) *Other documents and records as prescribed by regulators.*

Documents except mentioned above are retained as per Record and Documents Retention Policy of the Bank.

22. Awareness and Training on AML/CFT

All staffs shall be aware of the statutory and regulatory obligations on AML/CFT. Therefore, the Bank shall have both In-house and Out-house ongoing employee AML/CFT training program so that all staffs are adequately trained on the AML/CFT norms, policies/procedures. Training and assessment shall be done virtually, online or physically as per the need and situation. Staff shall be regularly updated upon any change of responsibilities and necessary job role. The training shall be focused on providing the risk-based approach, with explanation of the latest regulatory Guidelines, Corporate Governance, KYC and ML/TF/PF issues etc. AML Compliance Officer and Banks' concerned staffs working at AML CFT areas shall be sent for National and International level training programs.

The Bank shall arrange knowledge sharing program on latest developments on the AML/CFT issues to the shareholder holding shares above 2%, BOD and Senior Management. Bank shall also impart AML CFT Training to Remittance Super Agents/ Sub Agents regularly. Further, The Super Agents shall conduct AML CFT Training to their staff and sub-agents on regular basis and compliance of the same is monitored by AML CFT Unit.

23. Audit/Testing

Internal Auditor shall examine the AML CFT Program of the Bank and do inspection whether the AML/CFT System/mechanism is risk based or not and find out whether adequate system/mechanism for monitoring is done on financial action taken, PEP/PIP, High Risk Countries, Region and high risk products, high risk instrument, services and transactions etc. as per the directive. Internal Audit shall be carried out in the Bank (including their Branches / Units) at least once in a year to specifically check and verify application of CDD procedures and highlight shortcomings in AML/CFT/KYC issues, if any. Outcome of the Audit shall also be brought to the notice of the Audit Committee and AML CFT Committee of the bank.

PART C – MISCELLANEOUS

24. One off transaction:

Opening of account for 'one off' transaction must be avoided. If such transaction occurred, the same shall be reported to designate Compliance Officer at Head office, with proper justification as to why the opening of such account is authorized at branch level. Or prior to authorizing to open such account, clearance from Business unit/central operations shall be obtained.

25. Account Closed within three months:

Request to close an account within three months of opening would be reported to the designated KYC Compliance Officer at Branch with full details. The KYC Compliance Officer at Branch should review the reasons and give consent for closing the account prior to processing such request. Branch shall obtain declaration from the client stating exact/ real reason for the same including purpose of opening account in the first place. Branch shall report/notify of such closure to CICD, Head office for necessary review the same day.

26. Modern Slavery and Human Trafficking (MSHT)

Himalayan Bank is always against modern slavery and human trafficking in any form and in any place. Implementing a modern slavery and human trafficking policy in a bank involves to identify, prevent and address such issues by proper CDD of customer and ongoing monitoring of transaction and profile.

27. Payable Through Account (PTA):

The bank shall not allow direct use of its correspondent bank account by third parties for any transaction on its own behalf. The bank does not provide PTA (Payable Through Account) facilities to any of its customers including correspondent partners.

28. Commitment of Senior Management

Senior management of the bank is fully committed to establishing appropriate policies, procedures and controls for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. Senior management also commits to ensure that ML/FT/PF risks are understood and appropriately mitigated in the bank. It shall also ensure that effectiveness of controls shall be regularly reviewed. The senior management of the bank shall promote compliance as a core value and culture of the bank and the bank shall not enter into, or maintain, business relationships that are associated with excessive ML/TF/FP risks which cannot be mitigated effectively.

29. Non-Compliance with Bank's AML/CFT Policy and procedures

Any staff failing to abide by the policy and procedures set by the Bank to prevent money laundering, terrorist financing and Financing of Proliferation, shall be treated as a disciplinary issue. Any deliberate breach shall be viewed as gross misconduct. This could lead to termination of employment and could also result in criminal prosecution and imprisonment.

30. Regulatory Obligations

The Bank would be obligated to comply with all the prevailing legal, regulatory and institutional requirements.

31. Tipping Off (ALPA: 44 A)

Any information provided to the Financial Information Unit or disseminated to staff or representative while in normal course of business or in the process of providing it to any Investigating Units should not be disclosed to anyone except mandatory as per the prevailing law.

Any employee who tips off the customer that their account is under surveillance should be held liable for disciplinary action as per staff bylaws of the Bank.

32. Protection for Directors/Compliance Officers/Employees

In case if any loss occurs to anyone because of submission of information to the FIU or any Government or other Entity by staff and officials of the reporting Branch/Department. The reporting person would not be

held liable for such consequences and the bank would take the responsibility of covering all costs to defend him or her, legally.

Any employees or directors are exempt of criminal and civil liability for breach of any restriction on disclosure of information by contract or by any legislative, regulatory or administrative provision, if they report their suspicion in good faith to FIU or any government or other entity. This provision is available even if they did not know precisely what the underlying criminal activity was and regardless of whether illegal activity actually occurred.

33. Customer Awareness:

To achieve AML/CFT and KYC objective of the Bank, proper customer education/awareness and corporation is very essential. The Bank shall try to educate to the customers and make them aware and knowledgeable regarding the importance and seriousness of ML/FT/PF risk to the Bank and ultimately to its customers through front line staff/business units.

34. Code of Conduct of Employees/BOD:

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

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

35. Authority to Formulate Necessary Manuals/Guidelines

The CEO is authorized to approve appropriate Manuals/Guidelines required for the effective implementation of the provisions of this policy. Such Manuals/Guidelines shall be construed as the part of this policy and shall be read in conjunction with the provisions contained in this policy. There shall not be any contradiction in the Manuals/ Guidelines with this policy and any contradiction in the Manuals/Guidelines with this Policy shall be ab initio void to the extent of contradiction. The Manual/Guidelines shall be approved by the CEO and the same shall be furnished to the Board for information.

36. Retrospective Application

The standards set by this policy document apply to both new and existing business relationships. It is therefore necessary to initiate corrective actions on customer identification and customer due diligence as per this policy.

37. Repeal and savings

This Policy shall repeal erstwhile "AML/CFT/KYC Policy 2023". Anything done under previous policy shall be deemed to have been conducted under this policy subject to retrospective application wherever requires.

PART D – ROLES AND RESPONSIBILITIES

38.1 Roles and Responsibilities of Board

The Board of Directors is the apex and supreme authority of the Bank. BOD is responsible and accountable to frame and implement robust guidelines and frameworks for effective compliance with the laws of land and with the regulations and directives issued by the regulatory authorities. The illustrative but not exhaustive roles and responsibilities of the Board related to this Policy are as follows:

a) *The Board of Directors shall be responsible for forming the AML /CFT Committee under the BOD consisting of its directors to look monitor the AML/CFT unit progress and status on close*
b) *The Board shall be responsible for approving the policies ensuring the appropriateness, sufficiency and effectiveness of the policies adopted by the bank based on the overall risk level of the bank on prevention of money laundering and financing of terrorism. Also, the board shall ensure that the Policy Framework is comprehensive for key business and support functions and establish a method for monitoring compliance of the same.*
c) *The Board shall review the status of implementation of Anti Money Laundering Act, 2064, Anti Money Laundering Rules, 2073, and the provisions contained in the Directives/Circulars issued by NRB*
d) *The Board of Directors of the bank shall, at least on quarterly basis, discuss on setting up and improving mechanisms to prevent customer's suspicious and abnormal transaction or money laundering and make necessary arrangement for this effect.*
e) *The Board shall issue appropriate instructions to the senior management regarding proper implementation of AML Programs to comply with the regulatory requirement.*
f) *Any amendments / cancellation or revision in this policy shall be at the sole discretion of the Board.*

38.2 Roles and Responsibilities of AML /CFT Committee

The roles and responsibility of AML/CFT Committee shall be defined by the BOD as per the guidelines given by NRB in its TOR related to AML/CFT/KYC that broadly covers as follows among others-

a) *To review and update the BOD on status and progress on AML/CFT as per Asset (Money) Laundering Prevention Act 2064 (ALPA), Asset (Money) Laundering Prevention Rules 2073(Rules) and Nepal Rastra Bank (NRB) Directives No. 19.*
b) *To discuss on sufficiency of Policy, Procedure and framework, evaluation of its implementation and progress update/formulate suitable changes in AML/CFT/KYC policy, if required, as per ALPA, Rules and NRB Directives No. 19 and Financial Action Task Force (FATF) Recommendations.*

38.3 Roles and responsibilities of Risk Management Committee (RMC)

a) *Risk Management Committee is the Board level Committee which shall constantly monitor the nature of level of risk being taken by the Bank and how the risk relates to risk appetite and tolerance capacity of the Bank.*
b) *Ensure that adequate controls and systems are in place to identify and address AML CFT and operational risk.*
c) *Assess the quality and appropriateness of mitigation action.*

38.4 Roles and Responsibility of Operation Risk Management Committee

a) *To ensure that the bank's operational risk management has been clearly communicated to staff at all levels in the units that incur material operational risk. To translate operational risk framework established by the Board of Directors into specific policies, process and procedures that can be implemented and verified within the different business units.*
b) *To discuss on and adequacy of policies procedure related to operations AML/CFT/KYC issues*
c) *To develop mechanism to minimize risk related to operational issues on AML/CFT/KYC issues.*
d) *To discuss on the issues pointed out by Auditors related to AML /CFT/KYC.*

38.5 Roles and Responsibilities of Chief Executive Officer (CEO) and Senior Management

Chief Executive Officer is the head of the management which shall be primarily responsible for the implementation and ensure effective compliance of the Policies/procedure and guidelines of the Bank/Regulators. The illustrative but not exhaustive roles and responsibilities of Chief Executive Officer of the Bank related to this Policy are as follows:

a) *Circulate and implementation of the Policy approved by the Board.*

b) *The CEO shall ensure that the bank has all required procedural guideline in place to effectively achieve the objectives of this policy.*

c) *The CEO shall promote compliance as a culture and consider AML/CFT compliance as a basic ethic of doing business.*

d) *All the procedural guideline containing the controls, monitoring and reporting procedures shall be approved by the CEO.*

e) *The CEO shall also ensure that enough resources and required access to information, documents and staffs.*

f) *To review on quarterly basis as to whether or not the provisions of Anti-Money Laundering Act, and rules, directive, order or policy formulated under such act are complied with and submit a report to Financial Information Unit completing the review of the same in three months from the end of fiscal year.*

g) *The bank's senior management shall be responsible for identifying and managing the AML CFT compliance risk through all levels of the organization. The senior management shall discuss on the procedural aspects and adequacy of the Information Technology system adopted by the bank for identifying the ML, TF and PF activities and its prevention and also give suggestions to carry out AML function smoothly.*

38.6 Roles and Responsibilities of CICD:

CICD will check, monitor and report the compliance by the Bank on regulatory, legal and institutional requirements.

38.7 Roles and Responsibilities of AML/CFT Unit:

AML/CFT Unit will basically work under AML/CFT/KYC guidelines issued by NRB Directives no. 19, Related Act, International Practices and work outlined in TOR

38.8 Role and Responsibilities of Executive Operating Officer (EOO)

Executive Operating Officer means the Officer or such designated official having other titles of the Bank, who shall be responsible for overall Operations of the Bank.

Executive Operating Officer shall be responsible for ensuring proper implementation of this policy including checks and control and monitoring and reporting procedures across the Bank

38.9 Roles and Responsibilities of Branch Managers/ Department/Unit Heads

a) *Branch Managers/Department/Unit Heads shall be responsible, under the area of their control, for ensuring proper implementation of control, monitoring and reporting activities designed to prevent money laundering and terrorist financing.*

b) *Responsible to reasonably assure that staffs under their control have required knowledge and are not involved on any money laundering and terrorist financing activities.*

c) *To ensure all regulatory instructions are complied with.*

d) *To ensure to educate the staffs and pass all necessary instructions received from head office.*

e) *Implement AML CFT/KYC polices, and procedure as directed by management from time to time.*

38.10 Roles and Responsibilities of KYC Compliance Officers (at Branch Level and Head Office)

a) *KYC Compliance Officers (AML/CFT Implementing Officers) shall be responsible for executing the duties as required by various guidelines framed under this policy from time to time.*

b) *KYC Compliance Officers shall be primarily responsible for monitoring and detecting suspicious Transactions/Activities and report to AML CFT Unit.*

c) *The roles and responsibilities of KYC Compliance Officers shall be covered in their Job description and TOR given by Branch Manager or Department Heads or CEO.*

38.11 Roles and Responsibilities of Internal Audit Department

Internal Audit Department shall be responsible for check and review effectiveness of this Policy. The illustrative but not exhaustive roles and responsibilities of Internal Audit Department relate to this Policy are as follows:

a) *Internal Audit shall provide independent evaluation of compliance with this policy.*

b) *Internal Auditor shall be responsible for conducting checks and review regularly to ensure that the control and monitoring and reporting procedures under this policy.*

c) *Internal audit shall specifically check and verify the application of KYC/AML/CFT Policy and procedures at the branches/Departments and comment on the lapses observed.*

38.12 Role and Responsibilities of Human Resource Department *(HRD)*

Human Resource Department is responsible for managing overall human resources of the Bank. The illustrative but not exhaustive roles and responsibilities of Human Resource Department related to this Policy shall be as follows:

a) *HRD shall ensure that screening against sanction list and due diligence have been made before appointing any person in the permanent and contract positions in the bank.*

b) *HRD shall also ensure that due diligence of the employees is updated regularly, and record of KYE is maintained appropriately.*

c) *Assessment of adequate human resources requirement in AML CFT Unit, Branches and Departments for AML CFT Compliance.*

d) *Conducting AML CFT Training to all concerned*

38.13 Roles and Responsibilities of Individual Employees

a) *It shall be the responsibility of every individual employee of the bank to remain vigilant to the possibility of money laundering / terrorist financing risks through use of bank's products and services.*

b) *Any staff who come to know about the involvement of bank's staff or any of its customers in money laundering or terrorist activities must report to the higher management of the bank complying the standard procedure framed under this policy and shall be mandatory role of all staffs of the bank.*

38.14 Roles and Responsibilities of Reporting Cell

a) *Compile, check and send the report to different authorities as per their requirement.*

b) *Provide various reports to AML CFT Unit as per their requirement and ensure timely upload the report in SIS related to AML CFT Unit.*

38.15 Roles and Responsibilities of Legal Department

a) *Legal Department is responsible for keeping eyes on legal compliance of the Banking operation.*

b) *Providing legal opinion as and when required.*

c) *Providing recommendation on statutory and internal requirements on the need basis with regards to AML / CFT issues.*

38.16 Roles and Responsibilities of Central Operation

a) *Checking full compliance of AML CFT Policy and Manual at the time of on-boarding customers.*

b) *Customer identification and acceptance process to be followed as directed.*

c) *Not to open account for prohibited customer as highlighted in the policy.*

d) *Verify Customer screening is properly done and documented.*

e) *Verification of customer risk categorization*

f) *Verification of Beneficial Ownership Identification/Shareholding structure for Corporate Customer*

g) *Conduct GAP analysis for Customer information in CBS and update the same on regular basis*

h) *Ensure the customer information inputted properly in CBS*

i) *Review and update the Beneficial owners' details in CBS of all entity account*

j) Customer data cleansing/ purification in CBS

38.17 Roles and Responsibilities of Province Heads and Provincial KYC Compliance Offices

Province Heads and Province Offices are responsible for effective implementation of this policies in their respective Branches under province as a first line of defense. Proper resources including Human Resources to be managed by Province Offices to the Branches and ensure full compliance of this policy. Province Head shall arrange for periodic monitoring and control and arrange for corrective actions with highest priority in the Branches pertaining to their respective Provinces.

Part E: ANNEXURE

ANNEXURE 1: INDICATIVE LIST OF PEP/PIP

1. An indicative list of Politically Exposed Persons (PEP) and People in Influencing Positions (PIP):

1.1. Administrators/Politicians

- President, Vice Presidents
- Prime Minister and Incumbent ministers
- Central Working Committee members, District President and Secretaries of all national level political parties
- Both lower and upper house parliamentarians of federal parliament
- Speaker and Dy Speaker of House of Representative
- Chairman and Vice Chairman of National Assembly
- Cabinet Secretaries
- Special Class Government Officers and above
- Governors of provinces
- Chief Minister and Ministers of Provincial Government
- Speakers/Dy Speakers of Provincial Legislatures
- Mayors and Dy Mayors of Metropolitan Cities/ Sub Metropolitan Cities, Municipalities
- Chairman and Vice Chairman of Rural Municipalities
- Chief Election Commissioner and all Commissioners of Election Commission
- Auditor General
- Attorney General
- Chief and all members of Commission for the Investigation of Abuse of Abuse of Authority
- Chairman and all members of Public Service Commission
- Chairman and all members of National Human Rights Commission

1.2. Judiciary

- Chief Justice and Justices of Supreme Court
- Chief Judges of High Courts and District Courts

1.3. Army

- General and above rank

1.4. Police (Nepal Police, Armed Police Force and National Investigation Department)

- Deputy Inspector General (DIG) of Police and above rank.

1.5. Government Entities/Corporations (Fully or partially owned by Govt)

- Chairman
- Chief Executive Officers

ANNEXURE 2: INDICATIVE LIST FOR RISK CATEGORIZATION

1. Low Risk

Followings are the indicative list of Low Risk customers:

- Public sector enterprise fully owned by Government of Nepal.
- Ministries, Government Departments, Regulators, etc.
- Individual Customers with a regular source of income (salary, pension, rent, etc.)
- All Vostro accounts, Foreign Banks and Financial Institutions incorporated **except in FATF, high risk or grey list countries.**
- Self-employed individuals.
- Public limited company and its subsidiary listed in stock exchange.
- Individuals having income source as Social Security Allowances.
- International Charities and Non-Government Organizations that are operating for over 10 years with transparent working area
- UN Bodies
- Private Limited Companies/partnership firm/Sole proprietorship firm provided that their nature of business do not fall under high risk or medium risk category
- Any other customers other than those classified as High or Medium Risk

2. High Risk

Following are the indicative list of customers that can be categorized as High Risk:

- Person/outlet dealing with Gambling, Money exchange, Jewelry business, precious metals, precious products, Land broker (including firm/company doing real estate business), dealers in high value commodities
- Non-Financial Institution that carry financial transactions (Money Transmitters)
- Cash intensive/oriented business (such as tolls, gaming companies, casinos, Petrol Pumps etc.)
- Antique Dealers, Money Service Bureau and Dealers in arms.
- Accounts of bullion traders i.e. gold/silver/diamond and gems/jewelers.
- Politically Exposed Person or People in Influencing Positions (mentioned in **Annexure – 1)**
- Immediate Family members and close associated of PEP/PIP **
- High net worth Customers
- DNFBPs like--Notaries, Lawyers, law firms, and Chartered Accountants, Audit Firms
- Trusts, Charities, Religious Institutions, INGOs/NGOs and organizations receiving donations from abroad (other than those promoted by UN or its Agencies or with transparent working areas)
- Customers based in high risk countries/jurisdictions as identified by FATF
- Investment Management Companies, Money Management Companies and or personal investment companies
- Individuals with dubious reputation as per available public information
- Foreign National individual Customers except Indians.
- If Beneficial owner is PEP/PIP/HR and hold more than 50% shares.
- Joint account if any one of account holder is categorized as HR.
- Travel/Tours/Trekking Agencies
- Vehicle Sellers and recondition houses (Four wheelers)
- Embassy/Consulate Office including Ambassador/consular
- Accounts of Political Parties
- Manpower companies
- Local entities that deal with the entities located in tax heaven jurisdiction
- Any other customers that do not fall in either in low or medium Risks

****Immediate Family Members of PEP/PIP; Spouse, Children,** Parents, In-laws, Unmarried Siblings, Grandparents and grandchildren.

****Close Associate of PEP and PIP:** A person who maintains close relationship with the PEP or PIP and includes a person who is in a position to conduct substantial domestic and international financial transactions on the PEP's or PIP's behalf.

3. Medium Risk

Followings are the indicative list of Medium Risk customers:

- Non-Banking Finance Companies (e.g. Insurance companies, cooperatives etc.)
- Builders/Contractors other than involved in real estate business
- Stockbrokers
- Non-resident Nepalese (NRN)
- Refugee
- All Himal Remit Saving Accounts- till the time all the required documents are obtained and verified.
- All the accounts opened on the basis of application received online- till the time all the required documents are obtained and verified.
- All customers that do not fall in either in Low or High Risks
- **Indian Nationals and entities with more than 50 % shareholdings of Indian nationals.**
- **Some of the existing foreign nationals as defined in AML CFT Manual.**

Note: The list above is for indicative purpose only and not exhaustive. Furthermore, these cannot be used as mutually exclusive benchmarks to categorize a customer e.g. a local resident can have large cash source and therefore it should be dealt as high risk unless the case justifies otherwise due to some other reason/s.

ANNEXURE 3: EXAMPLES (SCENARIOS) OF UNUSUAL ACTIVITIES/TRANSACTIONS

Any one or a combination of the following transactions may indicate the act of money laundering. The list of situations given below is intended mainly as a means of highlighting the basic ways in which the money may be laundered. This list is by no means exhaustive and will require constant updating and adaptation to changing circumstances and new methods of money laundering. As it is solely an aid, it must not be applied as a routine instrument in place of common sense.

The employees need to be cautious if they encounter the following situations/ transactions and immediately report to the branch manager

1. Transactions that do not make economic sense

a) Transactions whose form suggests that they might be intended for an illegal purpose, or the economic purpose which is not clear/visible.
b) A customer-relationship with the bank that does not appear to make economic sense for e. g. a customer having many accounts with the same bank, frequent transfers between different accounts or exaggeratedly high liquidity.
c) Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawn.
d) Transactions that cannot be reconciled with the usual activities of the customer of the bank.
e) Transactions, which without plausible reason, result in the intensive use of what was previously a relatively inactive account.
f) Transactions, which are incompatible with the bank's knowledge and experience of the customer or with the purpose of the business relationship.
g) Provisions of bank guarantees or indemnities as collateral for loans between third parties that are not in conformity with market conditions.
h) Unexpected repayment of an overdue credit without any plausible explanation and back-to-back loans without any identifiable and legally admissible purpose.

2. Transactions involving large amount of cash

a. Exchanging an unusually large amount of small-denomination notes for the same amount in large denomination notes.
b. Frequent changing of large amounts of money without using a customer account and frequent withdrawal of large amounts by means of cheques, including travelers' cheques.
c. Frequent withdrawal of large cash amounts, which do not appear to be justified by the customer's business activity.
d. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash rather than by way of debits and credits normally associated with the normal commercial operation of the company, e. g. cheques, letter of credit, bills of exchange etc.
e. Depositing cash by means of numerous credit-slips by a customer such that the amount of each deposit is not substantial but the total of which is substantial.
f. The deposit of unusually large amounts of cash by a customer to cover requests for banker's draft, money transfers, or other negotiable and readily marketable money instruments.

3. Transactions involving abroad transfers

a. Transfer of money abroad by an interim customer in the absence of any legitimate reason.
b. A customer who appears to have accounts with several banks in the same locality, especially when a bank is aware of regular consolidated process from such accounts prior to a request for onward transmission of the funds elsewhere.
c. Repeated transfers of large amounts of money accompanied by the instructions to pay the beneficiary in cash.
d. Large and regular payments that cannot be clearly identified as bona fide transactions, from and to countries associated with the production, processing or marketing of narcotics or other illegal drugs.

4. Transaction involving authorized institution, employees and agents

a) Changes in employee characteristics, e. g. lavish life styles.
b) Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

5. Investment related transactions

a. Purchase of securities to be held by the Bank in safe custody, where this does not appear appropriate, given the customer's apparent standing.
b. Back-to-back deposit/ loan transactions with subsidiaries of, or affiliates of, overseas financial institutions known in drug trafficking areas.
c. Request by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.
d. Larger or unusual settlements of securities transactions in cash form.
e. Buying and selling of a security with no discernible purpose or in circumstances, which appear unusual.

6. Transaction of secured and unsecured lending

i. Customers who repay overdue loans unexpectedly.
ii. Request to borrow against assets held by institution or a third party, where the origin of the assets is not known, or the assets are inconsistent with the customer's standing.
iii. Request by a customer to the Bank for proving or arranging large finance where the purpose of such finance is unclear.

7. Transactions involving unidentified parties

i. Provision of collateral by way of pledge or guarantee without any discernible, plausible reason by third parties unknown to the bank and who have identifiable close relationship with the customer.
ii. Transfer of money to another bank without indication of the beneficiary.
iii. Payment orders with inaccurate information concerning the person placing the orders.
iv. Use of pseudonyms or numbered accounts for effecting commercial transactions by enterprises active in trade and industry.
v. Holding in trust shares in an unlisted company whose activities cannot be ascertained

8. Trade Based Money Laundering (as per FATF definition)

 A trade entity is registered at an address that is likely to be a mass registration address, e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, especially when there is no reference to a specific unit.
 The business activity of a trade entity does not appear to be appropriate for the stated address, e.g. a trade entity appears to use residential properties, without having a commercial or industrial space, with no reasonable explanation.
 A trade entity lacks an online presence or the online presence suggests business activity inconsistent with the stated line of business, e.g. the website of a trade entity contains mainly boilerplate material taken from other websites or the website indicates a lack of knowledge regarding the particular product or industry in which the entity is trading.
 A trade entity displays a notable lack of typical business activities, e.g. it lacks regular payroll transactions in line with the number of stated employees, transactions relating to operating costs, tax remittances.
 Owners or senior managers of a trade entity appear to be nominees acting to conceal the actual beneficial owners, e.g. they lack experience in business management or lack knowledge of transaction details, or they manage multiple companies.
 A trade entity, or its owners or senior managers, appear in negative news, e.g. past money laundering schemes, fraud, tax evasion, other criminal activities, or ongoing or past investigations or convictions.
 A trade entity maintains a minimal number of working staff, inconsistent with its volume of traded commodities.
 The name of a trade entity appears to be a copy of the name of a well-known corporation or is very similar to it, potentially in an effort to appear as part of the corporation, even though it is not actually connected to it.
 A trade entity has unexplained periods of dormancy.
 An entity is not compliant with regular business obligations, such as filing VAT returns. This may also include the address of a trust and company service provider that manages a number of shell companies on behalf of its customers.
 Trade activity is inconsistent with the stated line of business of the entities involved, e.g., a car dealer is exporting clothing or a precious metals dealer is importing seafood.
 A trade entity engages in complex trade deals involving numerous third-party intermediaries in incongruent lines of business.
 A trade entity engages in transactions and shipping routes or methods that are inconsistent with standard business practices.
 A trade entity makes unconventional or overly complex use of financial products, e.g. use of letters of credit for unusually long or frequently extended periods without any apparent reason, intermingling of different types of trade finance products for different segments of trade transactions.
 A trade entity consistently displays unreasonably low profit margins.5 in its trade transactions, e.g. importing wholesale commodities at or above retail value, or reselling commodities at the same or below purchase price.
 A trade entity purchases commodities, allegedly on its own account, but the purchases clearly exceed the economic capabilities of the entity, e.g. the transactions are financed through sudden influxes of cash deposits or third-party transfers to the entity's accounts.
 A newly formed or recently re-activated trade entity engages in high-volume and high value trade activity, e.g. an unknown entity suddenly appears and engages in trade activities in sectors with high barriers to market entry. In some cases, determining the profit margin may require estimating the "fair price" of the traded commodity, which may be difficult for certain types of commodities (e.g. commodities not traded on the open market).
 Inconsistencies across contracts, invoices or other trade documents, e.g. contradictions between the name of the exporting entity and the name of the recipient of the payment; differing prices on invoices and underlying contracts; or discrepancies between the quantity, quality, volume, or value of the actual commodities and their descriptions.
 Contracts, invoices, or other trade documents display fees or prices that do not seem to be in line with commercial considerations, are inconsistent with market value, or significantly fluctuate from previous comparable transactions.
 Contracts, invoices, or other trade documents have vague descriptions of the traded commodities, e.g. the subject of the contract is only described generically or non specifically.
 Trade or customs documents supporting the transaction are missing, appear to be counterfeits, include false or misleading information, are re submission of previously rejected documents, or are frequently modified or amended.
 Contracts supporting complex or regular trade transactions appear to be unusually simple, e.g. they follow a "sample contract" structure available on the Internet.
 The value of registered imports of an entity displays significant mismatches to the entity's volume of foreign bank transfers for imports. Conversely, the value of registered exports shows a significant mismatch with incoming foreign bank transfers.
 Commodities imported into a country within the framework of temporary importation and inward processing regime are subsequently exported with falsified documents.
 Shipments of commodities are routed through a number of jurisdictions without economic or commercial justification.

9. Miscellaneous transactions

- Purchase or sale of large amounts of precious metals by an interim customer.
- Purchase of bank cheques on a large scale by an interim customer.
- Extensive or increased use of safe deposit lockers, which do not appear to be justified by the customer's personal or business activities.
- Cash payments remitted to a single account by a large number of different persons.
- Request by a customer for investment management services where the source of funds is unclear or not consistent with the customer's apparent standing and,
- Request by a customer for a financial institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear.