AML/CFT/KYC
Policy
2022

(Approved by BOD meeting #423 dated 04 September 2022)

1st Policy- June 2014
Second Revision- November 2017
Third Revision- December 2018
Forth Revision- January 2020
Fifth Revision- June 2021
Sixth Revision- September 2022

HBL हिमालयन बैंक लिमिटेड Himalayan Bank Ltd.

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

Table of Contents

Heading No.	Heading	Page No.
1.	Abbreviations	4
2.	General Provisions	5
3.	Preamble	6
Part A	**General Information /Definitions**	**7-12**
Part B	**Bank's Policy and Procedure to Prevent ML and TF**	**13-35**
1	Objective of the policy	13
2	Know your customer Policy	13
2.1	Customer Identification procedure	13
2.1.1	Natural Person	14
2.1.2	Legal Entity	14
2.1.3	Multiple Banking Declaration	14
2.1.4	Physical Present	14
2.1.5	Mandate	14
2.1.6	Background/ information of customer	15
2.1.7	KYC update interval	15
2.1.8	Collection of Thump print	15
2.1.9	KYC of Walk in customers	15
2.2	One off transactions	16
2.3	Account closed within 3 months	16
2.4	Exception to customer identification	16
2.5	Specific identification issues	16
2.6	Simplified KYC/CDD	17
2.7	Corporate Account	17
2.8	PEP/PIP	17
2.9	Negative news alert	18
3.	Correspondent banking relationship	18
4.	Refusal of Account Opening Request	19
5.	Identification and verification by third party	19
6.	Customer Acceptance Policy	19
7.	Ongoing Customer Transaction Monitoring Procedure	20
7.1	Special monitoring of certain transactions	20
7.2	Monitoring Mechanism of Electronic Card Transactions	20
8.	Recognition and reporting of Suspicious /unusual transaction to FIU and other concerned authority	21
9.	Threshold Transaction Report	22
10.	Relaxation of sending particulars to FIU	22
11.	Sanction list update ALPA	22
12	Special provision on freezing of property	22
13.	Risk Management	23
14.	Risk Management through three lines of defense	23
15.	Country Risk	23
16.	Customer Risk	24
17.	Services Risk	24
18.	Risk Categorization review interval	24
19.	Internal Control	24
20.	Commitment of Senior Management	25
21.	Prohibited customers and transactions	25
22.	Opening Account and required documents	26
23.	Acceptable Identification Documents	26
24.	Categorization of accounts based on inherent risk	27
25.	Customer Risk Profile	27
26.	Certification of documents	27

27.	Monitoring Graded Accounts	28
28.	Detection of other possible money laundering transactions	29
29.	Wire/Electronic Transfers	29
30.	Terrorism Finance	31
31.	Trade Base Money Laundering	32
32.	Resubmission Policy	32
33.	Money Laundering in credit	32
34.	Introduction of new Technology/Products	32
35.	Tipping Off	32
36.	Complete Record Keeping	33
37.	Awareness and Training of Staff	33
38.	Risk Management (ALPA 7D)	34
39.	Non Compliance with Bank's AML/CFT/KYC policies and procedure	34
40.	Regulatory obligations	34
41.	Fraud Detection	35
Part C	**Roles and Responsibilities**	**36-40**
Part D:	**ANNEXURES**	**41-54**
1	Indicative List of PEP/PIP and Immediate Family Members and close Associates of PEP/PIP	41
2	Indicative List of Risk Categorization	42
3	Examples (Scenario) of Unusual Activities/Transactions	44
4	AML CDD Review Questionnaire for Correspondent Banks/FIS/Vostro Partners	47
5	AML/CDD Review Questionnaire for Principal Agents	50
6	AML/CDD Review Questionnaire for Himal Remit Subagents	52
7	ALPA Provision on Terrorist, Terrorist Group…...	53

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
CIF	CUSTOMER IDENTIFICATION FORM
CIP	CUSTOMER IDENTIFICATION PROCEDURE
CO	COMPLIANCE OFFICER
CTMP	CUSTOMER TRANSACTION MONITORING PROCEDURES
ECDD	ENHANCED CUSTOMER DUE DILIGENCE
EOO	EXECUTIVE OPERATING OFFICER
FATF	FINANCIAL ACTION TASK FORCE
FIU	FINANCIAL INFORMATION UNIT
HBL	HIMALAYAN BANK LTD.
KYC	KNOW YOUR CUSTOMER
ML	MONEY LAUNDERING
NID	NATIONAL IDENTIFICATION DOCUMENT
PEP	POLITICALLY EXPOSED PERSON
PIP	PEOPLE IN INFLUENCING POSITION
PTA	**PAYABLE THROUGH ACCOUNTS**
RM	RISK MANAGEMENT
STR	SUSPICIOUS TRANSACTION REPORT
TF	TERRORIST FINANCING
TTR	THRESHOLD TRANSACTION REPORT
TBML	**TRADE BASED MONEY LAUNDERING**

2. GENERAL PROVISIONS

This Policy represents the basic standards of Anti-Money Laundering and Combating Terrorism Financing (hereinafter referred to as AML/CTF), 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 and procedures to prevent Money Laundering and Terrorist Financing
Part C : Duties and responsibilities
Part D: 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) and Terrorist Financing (TF).

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 (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 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 guideline provided by Central bank (Nepal Rastra Bank), FIU, and under preview of "Asset (Money) Laundering Prevention (Second Amendment) Act, 2014" **(ALPA**) promulgated by the parliament, Anti Money Laundering Prevention Rules 2073 (October 2016) and Directive issued by Financial Information Unit (FIU) and Nepal Rastra Bank (NRB) 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 and **such changes can be approved by the Management.**

PART A: GENERAL INFORMATION/DEFINITIONS

1) **AML/CFT Committee** is committee formed under the BOD to monitor/review the status of AML/CFT/KYC issues of the bank.
2) **AML/CFT Unit** is a unit formed under compliance department reporting to AML CFT Committee and CICD parallelly, to look after AML/CFT/KYC issues of Bank on full-fledged manner
3) **The Bank** means Himalayan Bank Ltd and
4) **The Board** means Board of Directors of Himalayan Bank Ltd
5) **Chairman** means the Chairman of the Board of Directors of Himalayan Bank Ltd
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.
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.
8) **Compliance Department** is the Department which looks after overall compliance and internal control of the bank
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.
10) **Walk in customer:** A customer who does not have account with us but avails services from the bank for himself or for others.
11) **Branch Managers** means heads of branches of the Bank.
12) **Dy Branch Managers** is Branch Manager who is 2nd head in the branch.
13) **Alternate Branch Manager**: Who works in absence of Branch Managers.
14) **Department Head** means the head of a particular department of the Bank.
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.
16) **Reporting Cell** is the department which collects, compiles, verify all the reports to be sent to central bank and other concerned department.
17) **RMC** refers to the Board level Risk Management Committee of the Bank.
18) **Legal Department** means the Department formed to ensure legal matter related to various laws and regulations on behalf of Banks.
19) **AML/CFT Policy** refers to "Policy for Prevention of Money Laundering and Combating the Financing of Terrorism. Act", "Rules" and "Directive" refer to the Asset (Money) Laundering Prevention Act 2064 and its latest amendment, Asset (Money) Laundering Prevention Rules 2073 and "Directive" will refer to the directive issued from Nepal Rastra Bank and Financial Information Unit.
20) **Legal (Entity) Person**: 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.

21) **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.

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

23. Domestic High-Profile Person/ Domestic Politically Exposed Persons (PEP) and People in Influencing Position (PIP)

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.

As per this policy, indicative list of Domestic High Profile Persons/Politically Exposed Persons or People in Influential Position and their family members along with close associates have been as illustrated in Annex 1.

24. High Net worth Individual: Shall be fixed by the management from time to time.

25. Foreign High-Profile person/Foreign politically exposed person

Politically exposed person who is or has been the Heads of State or of government, senior politician, central member of national political party, senior government, judicial or military official, senior executives of state-owned corporations of a foreign country.

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.

27. Asia Pacific Group on Money Laundering (APG)

Asia/Pacific Group on Money Laundering (APG) 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.

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". The paper aims to provide customer identification and know your customer framework for banking supervisors based on which they can help establish/develop practices for the banks and financial institutions to design their own KYC programs. 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.

29 Financial Information Unit (FIU)

FIU, an independent body established by the Government of Nepal in accordance with "Asset (Money) Laundering Prevention Act 2008", enacted on 28 January 2008 to regulate and prevent money laundering activities in Nepal in line with international norms.

30. Money Laundering (ML)

30 .1 Money Laundering/Combating for Financing Terrorism

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.

30.1.1 Stages of Money Laundering

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.

30.1.1.1 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

30.1.1.2 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.

30.1.1.3 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.

31. Customer Due Diligence (CDD) :

Customer Due Diligence (DD) 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. CDD is the process of identifying (CIP) and evaluating the customers and the assessment of customers risk as part of KYC.

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.

33. Know Your Customer (KYC)

Know your customer (KYC) is the due diligence and regulation that Banks must carry out to identify their customers and ascertain relevant information for carrying out financial transactions with them.

One of the key aspects of KYC is to verify that a customer/prospective customer is not enlisted as a fraudster, terrorist, money launderer or regarded as high-risk or carries negative report in media/public records.

33.1 Simplified KYC/*Simplified Customer Due Diligence (SCDD) :*

This can be conducted for customers who fall under low risk customers having characteristics as specified by NRB directive i.e. whose total annual deposit or transactions remain within the limit of NPR 100,000. HBL context, Earthquake Account, Social Security Account, Mero Pahilo Khata etc or as specified by NRB.

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. Separate forms shall be developed and collected details about Employees of the organization by Human Resource Department.

HBL Staff Bylaws with Code of conduct has been vital documents for addressing HR issues of the organization.

Additionally, KYC of Intern hired by the bank also to be obtained and to be on record with google map of location and contact number.

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 Annex- 2 which shall be updated from time to time.

36. Shell Entity

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 havens.

"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.

37. 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 of Nepali origin, born residing outside Nepal.

38. Compliance Officer(s)/KYC Officer 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/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.

39. 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.

40. 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.

41. Sanction Programs:

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. 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.

HBL has its own Swift Sanction Screening software to screen **cross border wire transfers.**

42. 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 creating 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.

43. 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 bona-fide 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

44. Suspicious Transaction Report:

A report to be made by Financial Institutions to Financial Information Unit on any suspicious transactions or any attempts under the provisions of "Parichhed 3, 7dha- Asset (Money) laundering prevention Act 2064" and point no. **14** of NRB Directive no. 19.

45. 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.

46. FATCA Reporting:

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

47. 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.

48. Egmont Group:

The **Egmont Group of Financial Intelligence Units** is an informal network of **167** financial intelligence units (FIUs) as of **June 2022**. National FIUs collect information on suspicious or unusual financial activity from the financial industry and other entities or professions required to report transactions suspected of being money laundering or terrorism financing. FIUs are normally not law enforcement agencies, with their mission being to process and analyze the information received. If sufficient evidence of unlawful activity is found, the matter is passed to the public prosecution agencies.

49. 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.

Himalayan Bank is always against modern slavery and human trafficking in any form and in any place.

50. 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. Bank does not provide PTA facilities to any of its customers including corespondent partners.

PART B: BANK'S POLICY TO PREVENT ML AND TF

1. 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 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. The core objectives of this policy are-

i. to prevent the bank mainly from being source/ platform to channel monies 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 CFT.

2 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)

2.1 Customer Identification Procedures (CIP) (ALPA: 7A)

CIP is a process of identifying the customer and verifying his/her/their identity by using reliable, independent supporting documents or data or information, including that available in third party-database. The designated staff must obtain enough information to establish the identity of each new customer along with the intended purpose of the relationship. Customer Identity shall be accurately identified when carrying out the following acts:

i. establishing business relationship,
ii. opening an account,
iii. carrying out occasional transaction above the threshold,
iv. carrying out fund transfer by electronic means,
v. suspicion about the veracity or adequacy of previously obtained customer identification information,
vi. suspicion of money laundering or terrorist financing,
vii. performing transaction(s) anytime in relation to the high risk and politically exposed person,

CIP is carried out to satisfy the Bank and other competent authorities that due diligence process has been carried out based on the risk profile of the customer and checked potential risk associated with it. Such risk-based approach is considered necessary to avoid disproportionate cost to the institution and

burdensome process to the customers. Besides the risk perception, nature of information / documents required shall also depend on the risk category of the customer.

Branches and concerned departments, shall take following measure when undertaking the identification and verification of its customer.

i. understanding and obtaining information and detail clarifying on the objectives, purpose and intended nature of business relationships and transaction.
ii. where the customer is a legal person or legal arrangement, understanding and verifying its ownership and control structure **including Ultimate Beneficial Owner (UBO)**, and obtaining such information.
iii. when a person is establishing business relationship or conducting transaction on behalf of another customer, obtaining identification document of such person and the person working on behalf of him including evidence verifying that such person is properly authorized to act.

2.1.1. Natural person:

For the customer that is a natural person, the designated staff/ KYC 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

2.1.2. Legal Entity:

For the customer that is a legal entity, the designated staff/ 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.

2.1.3. Multiple banking declarations:

Multiple banking declarations must be obtained before providing loan to the natural person, firm, company or institution.

2.1.4. Physically present:

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 Officer at the Branch. It is the responsibility of the compliance Officer of Branch to ensure that such contact or meeting is held. The original identification document must be verified during the same process. Non Face to Face Account opening if any 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.

When it is not possible to have face to face contact/meeting and/or verify the original identification document during the account opening time, the authorized staff must note down the same on the application for account opening form. **Account debit is not permitted in such accounts however Face to face meeting with Representative Officer deputed in different countries is as good as face to face meeting with the concerned official of the Branches.**

Meeting through Video conference or any other digital media where the identify of the customers can be verified shall also be considered as Face to Face Meeting unless restricted by NRB.

2.1.5. 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. Thump 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**".

2.1.6. 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 black list and screening software to find out the background information of the customers.

Account Opening Form, **KYC Forms, CDD and EDD forms, Remittance Release Forms etc.** are used to collect those information.

Transactions on accounts shall be monitored for consistency with the expected normal activity as specified by the customer or subsequently updated by the Bank.

2.1.7. KYC update interval:

1. KYC update and beneficial owner identifications should be done as follows:

   Ka. Every year in case of high-risk customers
   In every 8 Years in case of Medium Risk Customers
   In Every 10 Years in case of Low Risk Customers.
   Every 10 years for customers applied with simplified KYC

   Kha. If transactions do not match with the KYC details- immediately.
   Ga. If KYC update not complete, immediately.
   Gha. If bank is suspicious about the true facts of KYC provided by the customers
   Kna. Bank shall **conduct EDD and update KYC o**f the high-risk customers annually.

2. On the basis of information received by bank officials about the customers officially or unofficially, judging the reality of information there should be arrangement to update KYC of customers.
3. Customers should be asked only the required and pending documents while updating KYC.
4. If KYC not possible even after putting much efforts, separate record should be kept for such customers. KYC can also be updated through **Telephone, mail or online or any other means.**
5. While doing customer identification and KYC Update, documents as listed in Annexure should be **obtained**. If felt necessary, additional documents **may be asked from the customer.**
6. While opening account of legal entity, audited balance sheet of last financial year to be obtained, then it can be obtained on the basis of risk associated with the entity. **(NRB Directive No. 19, serial 8, (7)**

2.1.8. Collection of Thump Print of customers on documents or through electronic Device:

While opening account of customers as per Assets ML Regulations Section 4, Thump Print of following individual shall be obtained:

a) For account of individual, if account operator and account holder is different, thump print to be obtained in case of mandatee.
b) In case of legal entity, Thump Print of account operator to be obtained **except for** Offices of Nepal Government, corporations/entity, group of companies under Government of Nepal, Bank and Financial Institution licensed by NRB., UN and offices under UN, intentional organization, Embassies
c) In case of staff of Government Institutions, account can be operated through their Office ID also.
d) Bank can collect Thump Print of customer on document or through Biometric based on risk

2.1.9. KYC of Walk in customers:

As per Assets ML Regulations 3, walking customer who deposit above Rs. 0.1M (one lac) or equivalent to FCY amount, identification of such customers with contact details should also be obtained.

Prepaid card users not having account with us: Full KYC to be obtained before issuance of Cards. Credit Card customer not having nominee accounts: Full KYC to be obtained and kept in record before issuance of cards.

Branches shall maintain a separate register consisting the list of customers with whom they are unable to establish contact in course of KYC update.

2.2. 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 Compliance Internal Control Dept shall be obtained.

2.3. Account Closed within three months:

Request to close an account within three months of opening would be reported to the designated Compliance Officer/KYC Officer at Branch with full transaction details except customers with high volume of transactions set by the bank. The 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 of such closure to CICD –/AML/CFT Unit, Head office for necessary review the same day.

2.4. 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 Compliance Officer of the Branch under intimation to the Head of Compliance Department/EOO at Head Office. Reason/s of such exception must be documented.

2.5. Specific Identification Issues: Identification of Customer's beneficial owner (ALPA 7C):

Branch should establish whether the customer is using name of another customer or person acting as a "front" or "on behalf" as trustee, nominee or other intermediary of the said person. If so, 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, identification of a trust should include the trustees, settlers/grantors and beneficiaries.

To establish the beneficial ownership, branches 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% of the customer
2. Who has effective control of the customer
3. The person on whose behalf transaction is conducted

2. While identifying the beneficial owner, following procedure to be followed.

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. Record and information as provided by legal entity.
e. Commercial Data base of companies
f. Information **received** from Nepal Government's concerned authorities/organization.

KYC officer/ Customer service staff/**Tellers** shall ascertain whether a person is acting or establishing business relationship or conducting transaction, on behalf of another person.

Wherever necessary additional information on beneficial ownership including disclosure from customer/ client that he/ she is rightful beneficial owner of particular transaction and being carried under full knowledge shall be taken. Full KYC of Beneficial Owner to be obtained and filed.
Mandate given in case of sole proprietorship company, full KYC including thump print to be obtained.

2.6 Simplified KYC/*Simplified Customer Due Diligence (SCDD)* : 7F of Act and Regulation No. 9:

(1) Bank may adopt a simplified CDD for identification and verification of a customer and transaction where the risk of money laundering or terrorist financing is identified to be lower.

(2) No such simplified measures of identification and verification shall be applied if there is suspicion of ML and TF.

(3) Other provisions regarding simplified KYC/CDD and its verification shall be as prescribed by NRB Directives.

However following accounts cannot be opened with simplified CDD:

1. If customer is foreigner
2. If customer is from country not complying aml rules or if customer's main transaction is with such high-risk countries
3. If customer is listed in stock exchange of high-risk countries not fully compliant with AML rules.
4. If true beneficial owner is not clear.
5. If customer or true beneficial owner is PEP/PIP
6. If customer is suspicious or doubtful.
7. If Transactions is above Rs. 1 lac

2.7 Corporate Account:

Staff 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.

Renewed KYC document including, latest tax **clearance certificate/ tax paid receipt**, audited balance sheet, change of shareholding pattern etc is obtained at the time of renewal of credit lines by respective RMs. If there is no credit lines, it shall be the responsibility of Customer Service in coordination with KYC Officer to obtain renewed documents including KYC every year of legal entity

Details of every natural/legal entity person having 10 % or more share **(Directly or indirectly through layers of legal entities)** or entertain voting rights, Partners of limited liabilities firms or similar firms or natural person who controls or has rights to control legal entities or a company, partnership firm with limited liabilities or similar types of firm should be taken.

2.8 Politically Exposed Persons (PEP) and People in Influencing Position (PIP) and Associates (ALPA:7B) (High Ranking Individual) s:

The Designated Compliance Officer in the Branch shall gather sufficient information from a new customer, verify with the updated list of PEP/PIPs and Associates and also check with publicly available information.

Bank shall establish a risk management system to identify whether a customer, person seeking to be customer, or a beneficial owner of a customer or transaction is politically exposed person.

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

a. Obtain approval from senior management **(EOO)** while establishing a business relationship
b. 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

Provisions stipulated in sub-sections (a) and (b) shall be applicable to the family members and associated persons of **domestic**/foreign **or international** PEP.

All types of PEP/PIP are considered as high risk.

Following process should be followed while identifying the PEP/PIP:

a. Obtain information from customer (declaration from customer)
b. Obtain information from new media.
c. Judge and keep tab of the news of social media.
d. **Obtain information from** Commercial Data base national international.
e. As per prevailing law record kept in any authority.
f. Record of pep/pip should be kept for 5 years from the date of their retirement from their positions.

The Compliance Officer at Head Office should be consulted in case of need regarding to take decision to open the account or continue the business relation with an existing PEP/PIP.

Provisions stipulated above shall also be applicable to the family members and associated persons of foreign or domestic PEP.

2.9 Negative news alert/Global/ Watch List Matches:

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 list and blacklisted customers of the Nepalese Industry. Branch shall screen all list provided by Software against sanction/pep/pip. Further, Branches and all concerned shall check CIB Blacklist to ensure non inclusion of individual/entity prior to establish any kind of relationship with the bank and then on periodic basis.

3. Correspondent Banking relationship (ALPA:7M):

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 the correspondent Bank's business. The Bank shall undertake such CDD on establishment of every 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 management, major business activities, and location of business, money laundering prevention and detecting efforts, purpose of the account, proper identification and CDD of third party using the correspondent banking.

Annual CDD is mandatory for Vostro Accounts, Nostro accounts with negative news and Remittance Agents Super Agents and Sub Agents. Principal Agents shall collect CDD of sub agents all over Nepal. The questionnaire as per Annex–4 should be obtained from Correspondent partners to gather sufficient information.

Principal Agents shall provide required CDD information/data of its sub agents and customers as and when required by the Bank.

The correspondent Bank or Financial Institution should not be a Shell Company or located in Non-Cooperating Countries and Territories categorized time to time by FATF or other FSRBsuch as APG. Approval of the senior management should be obtained before establishing new correspondent relationship.

Bank does not provide payable through account facilities to any of its customers including corespondent partners.

Transaction monitoring has to be done with the correspondent banks from time to time and check whether the business partner banks are following AML/CFT Rules and if not followed business should be stopped with such organization.

CDD of Vostro Accounts, Nostro Accounts, Remittance – Principal Agents and Correspondent partners shall be done in an annual basis.

4. Refusal of Account Opening Request (ALPA: 7 0):

When the staff designated to open new accounts finds sufficient ground that the customer is not disclosing the reason for opening account, transaction volume etc it shall be referred to the Branch Manager and Designated Compliance Officer (KYC OFFICER) in the Branch. The Designated Compliance Officer, after consultation with the staff and Branch Manager can refuse the request for account opening. 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 circulated to all the Branches for their reference not to entertain those customers refused by one Branch.

Before approving account opening of customers, the Designated staff/Compliance Officer/KYC Officer in the Branch shall verify legal status of the person / entity against and the relevant identification documents and-

shall verify that any person purporting to act on behalf of a legal person/entity is authorized to identify himself/herself, verify the identity of that person, understand the ownership and control structure of the customer and identify the natural person/s that ultimately control the account or legal entity.

a. shall check that the request is not from a Shell Company as Banks **does** not **establish any kind of relationship with** such companies (ALPA: 7).
b. shall immediately inform the Compliance Officer at the Head/Central Office if an account has been opened, but problems of verification arise which cannot be resolved. The account can be closed on such ground as well.
c. shall discuss the with Branch Manager and Compliance Officer of the Branch for the final decision that needs to be communicated to the customer where the designated staff of the Branch is unable to apply appropriate CDD measures due to non-submission of information and /or non-cooperation by the customer.
d. shall not open the account of Individual or entities listed in UN and OFAC sanctions list.
Rejection list is maintained by the Bank per AML CFT Manual.

5. Identification and Verification by Third Party (ALPA:7J)

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.

6. Customer Acceptance Policy (CAP)

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 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 (ALPA:6).
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, purchasing of foreign draft, transferring funds by any medium, accepting funds from any medium or carrying out transaction for the reasons as mentioned in Customer Service Manual of the Bank.
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. (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. Account opened with insufficient documents shall be marked as post no debit and no cheque book shall be issued against such accounts.

viii. All rules related to AML/CFT will applied whether customer account is opening through Centralized Level or through Online, keeping the required control while delivering cheque, screening before on-boarding, identification and acceptance of the customer.

7. Ongoing Customer Transaction Monitoring Procedures (CTMP) (ALPA:7I):

Bank shall regularly do ongoing due diligence as per 7.1

7.1 Special Monitoring of Certain Transactions 7: Bank shall pay special attention to the following: -

(a) all complex, unusual large transactions and all unusual patterns of transactions or which have no apparent economic or visible lawful purpose.

(b) business relationships and transactions relating to the customer and financial institution of a country internationally identified as a country that do not or insufficiently comply with AML/CFT international standards,

(c) such other transactions prescribed by the Regulator.

(f) Bank shall **check and regularly monitor** whether the electronic machine or cards is being used as per the information and guidelines of the banks While monitoring, if it is found to be suspicious, information to be given to FIU including other concerned authorities.

Ongoing monitoring is an essential element of effective CDD process. Customer transaction shall be monitored automatically or manually whichever is feasible for the bank.

Compliance Officers should pay special attention to all complex, unusually large value and/or unusual pattern of transactions that have no apparent economic or visible lawful purpose.

High-risk accounts including of money changers, real estate brokers, lawyers, notaries etc. shall be closely monitored. Bank conducts Enhanced Due Diligence (EDD) at the time of account opening and annually thereafter for High Risk Accounts.

They shall also put in place a system of periodic review of risk category of accounts and need for applying enhanced measures of due diligence. Furthermore, they shall ensure that a record of transactions in the accounts is maintained and preserved and any transaction of suspicious nature is immediately reported to the CICD- AML/CFT Unit at Head office **for further submission to FIU if required.**

Designated Compliance Officers (KYC Officer) shall ensure that their branch maintains proper record of all transactions of Rs.1 million and above.

The teller processing cash transaction of above Rs. 1 million shall obtain declaration from the customer about source and purpose of deposit.

Like wise, prior to approving cheque withdrawals of more than Rs. 1M, concerned Branch must obtain clearance from Central Operations.

Customers having high amount / value of cash transaction/s shall have to be identified by the Designated KYC Officer of the Branch and must be noted in the CDD form so that the tellers and supervisors are aware of the same. AML/CFT Unit designated staff at Head Office shall monitor/report various Accounts/Transactions as required by central Bank under Directive No. 19.

The Branches shall exercise ongoing due diligence 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 customers' 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 including PEP, high risk customer or of beneficial owner, their business relation, transaction in to ensure that the same are kept up-`to-date,

(d) monitor cross border correspondent banking and wire transfer and such customers,
(e) To perform other functions as prescribed by the Regulator and Bank.

7.2. Monitoring mechanism for transactions performed using electronic cards in PoS, ATM etc.

Roles of Business Unit

Card Center business unit generate daily transaction report of POS and e-com merchants every day and go through this report thoroughly for any unusual transactions. These unusual transactions include but are not limited to:

- **a) merchants with high volume/value of transactions than normal.**
- **b) transactions with no information**

If suspicious transactions are detected, Unit contacts the merchant and ask for the detail of these transactions such as, sales slip, invoice etc. If they are unable to justify the transaction then bank shall proceed for blocking the fund, suspension of account and report this transaction. If needed, transaction should also be confirmed with the issuer bank.

If any unusual transactions identified shall be referred to AML CFT Unit/CICD for further investigation/analysis.

Role of Transaction Analyst at AML CFT Unit

Transaction analyst shall investigate in detail about the transactions and shall raise STR/SAR if required in consultation with Head of AML CFT and Compliance Dept.

Further, transactions analyst shall also monitor through alerts generated by AML Software.

Besides, on quarterly basis, all the transactions done using electronic cards is analyzed by Transaction Analyst in AML CFT and identify unusual nature of transactions, if any.

If any SAR/STR is identified, then the same shall be reported in consultation with Head of AML CFT and Compliance Dept.

8. Recognition and reporting of suspicious transaction (ALPA:7 S)

The Compliance Officer of Head Office should report details of suspicious transactions to FIU in the format prescribed by FIU.

All the staff of the bank shall be personally obliged to report any unusual transaction suspecting to money laundering and terrorist financing activity to the Compliance officer, Head office as per Annexure in AML CFT Manual.

All staff must be continuously alert to identify/track unusual or suspicious transactions or activities viz. activity that appears to be inconsistent with the ones that have been declared by the customer or have a relation with drug trafficking / terrorism / other crimes, structuring of transactions to obscure/evade audit trails or identification or record keeping etc. some of the examples of the suspicious transaction are enlisted in Annex-3.

i. Branch Manager shall also be responsible to ensure that branch working under them are carrying out due diligence of transaction and they have reasonable information about the customer/ beneficial owner and their business and KYC forms are complete.
ii. The Bank shall fully cooperate with all law enforcement agencies and their investigations within the scope of applicable laws and in consultation with the Legal Department.
iii. In order to facilitate further inquiries by the concerned authorities all unusual transactions have to be handled with utmost care. The Bank shall never let the customer know about stage of the process.
iv. The Staff that fails to report unusual and suspicious transaction shall be construed as negligence in discharging entrusted duties and subject to disciplinary action in accordance to the staff by laws.

8.1. STR/SAR Decision Making Process

Transaction Analyst(s), Head of AML CFT Unit and Head of CICD shall discuss and take final decision whether to raise STR/SAR or not.

8.2 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, staff and officials of the reporting Branch/Dept. 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 or otherwise.

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. This protections is available even if they did not know precisely what the underlying criminal activity was and regardless of whether illegal activity actually occurred. (to vet with legal- language).

For transaction monitoring purpose, bank shall implement Transaction Monitoring Software.

Submission of STR has to be kept confidential and branches are cautioned against tipping off the customers who are being reported upon.

9. Threshold Transaction Report (TTR):

Bank shall report following limit of transactions to FIU within Fifteen (15) days of transaction **through goAML based on the TTR xml files generated by AML Software**-

i. Single or multiple CASH deposits by a customer in a day in Rupees of above One (1) million above limit set by the concerned authority from time to time.
ii. Single or multiple Cash withdrawal by a customer in a day in Rupees above One (1) million or limit set by the concerned authority from time to time.
iii. Single or multiple Wire Transfer by a customer in a day in Rupees above One (1) million or limit set by the concerned authority from time to time.
iv. Single or multiple Foreign Exchange of transactions by a customer in a day in Rupees above of Five (5) Hundred Thousand or limit set by the concerned authority from time to time.

Any cash transaction above threshold limit, declaration of source of fund should be disclosed by the customer in the deposit slip and same should be updated in Core Banking System (CBS).

10. Relaxation of sending particulars to FIU:

Relaxation/exception for TTR and STR shall be as per NRB Directives.

11. Sanctioned list update Alpa 6,2 , Section 29 5 .sub section 1 and 3. :

Authorized vendor providing sanctioned list of domestic and international PEP/PIP/Sanction list shall regularly updates the list.

Further AML CFT Unit/Compliance Department shall update the private list if any on periodic basis. All sanctioned list is screened through screening software which has updated list of sanctioned lists, at the time of opening new accounts as well as doing any new transactions.

Screening of existing customers against sanction lists is done on monthly basis as on going Screening.

12 **Actions and Freezing of Property and Funds against specially designated persons, groups and organizations in persuant to section 6 kha of the Act.**

(1) Natural Person, concerned agency, Bank shall immediately and without delay, freeze the property or funds of a person, group or organization listed pursuant to section 29E., 29F. and of person, group or organization engaged or financing in the proliferation of weapons of mass destruction.

(2) While freezing the property or funds in accordance with subsection (1), all the following property of fund shall be frozen: -

(a) All property or funds belonging to or wholly or jointly, directly or indirectly, owned or possessed or held or controlled by such person, group or organization,

(b) All property or funds derived or generated from the property or funds pursuant clause (a), 28 (c) All property or funds of a person, group and organization acting on behalf of, or at the direction of such person, group or organization.

(3) Natural or legal person, legal arrangement, concerned agency or reporting entity shall make necessary management that the property or funds frozen pursuant to subsection (1) and (2) shall not be, directly or indirectly, available or in use of or be beneficial to the terrorist, terrorist group or terrorist organization and also to the person, group or organization related with the proliferation of weapons of mass destruction or of its financing and that shall be frozen in such a way that such property or instrumentality could not be transferred, mortgaged or sold or distributed or transacted by anyone, except in the execution of the provision of this Act and rules there under.

(4) Natural or legal person, legal arrangement, concerned agency shall send the report of such freezing pursuant to subsection (1) and (2) to the Ministry of Finance and reporting entity to the Regulator within three days of freezing.

(5) Regulator shall submit the detail of the freezing of the property or funds received pursuant to subsection (3) to Ministry of Finance within three days.

(6) Other additional provisions regarding freezing of property or funds shall be as prescribed.

Please refer Annexure 7 for details about freezing of Fund or Property

13. Risk Management (RM) (ALPA:7D)

The Bank shall adopt a risk-based approach to the implementation of this Policy. 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. Followings are the risk criteria used to identify customers and transactions risk.

14. Risk Management through Three Lines of defense:

For the effective assessment, understanding, management and mitigation of ML/FT risks, bank shall adopt three line of defense. Identification and analysis of ML/FT risks and effective implementation of policies and procedures to encounter the identified risk is the feature 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:

Branches/Business Units and departments shall function as a first line of defense to prevent ML/FT risks. Business shall promote AML/CFT principles while doing business. Businesses shall own and manage the ML/FT risks arising from the business. Persons 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 compliance department to assist business units/departments in this process.

b. Second line of defense:

Compliance and internal control Department/AML CFT Unit shall function as a second line of defense to prevent ML/FT risks in the bank. The Compliance Department shall monitor overall legal, regulatory and internal compliance of policies, procedures and guidelines. It shall also provide required regulatory compliance expertise and guidance, set standards and trainings for businesses to manage and oversee ML/TF risks.

c. Third line of defense

This shall be performed by 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.

15. Country Risk:

Factors that may result in a determination that a country poses a higher risk include:

ι. Countries subject to sanctions, embargoes or similar measures

ιι. Countries identified by the Financial Action Task Force (“FATF”) as **"High-Risk Jurisdictions subject to a Call for Action"**

ιιι. Countries identified by credible sources as providing funding or support for terrorist activities.

ιϖ. Countries identified by credible sources as having significant levels of corruption, or non-transparent tax environment.

16. Customer risk:

There is no universal consensus as to which customer poses a higher risk. However, characteristics of customers have been identified with potentially higher money laundering risks and are listed in **Annexure 2 as an indicative List of Risk Categorization.**

17. Services risk:

Determining the money laundering risks of services should include a consideration of such factors as:

- **i.** Services identified by regulators, governmental authorities or other credible sources as being potentially high risk for money laundering,
- **ii.** Services involving banknote and precious metals trading and delivery.

18. Risk categorization review interval:

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

19. Internal Control:

BOD shall formulate and develop necessary, policy, procedure or controlling systems on the basis of "Asset (Money) Laundering Prevention (Second Amendment) Act, 2014" **(ALPA**) promulgated by the parliament, Anti Money Laundering Prevention Rules 2073 (October 2016) and AML Directives from Central Bank.

Bank shall appoint compliance officer at management level to comply the obligation pursuant to the provision of under preview of "Asset (Money) Laundering Prevention (Second Amendment) Act, 2014" **(ALPA**) Anti Money Laundering Prevention Rules 2073 (October 2016) and AML Directives issued by Central Bank.

Bank ensure the following powers and necessary resources for compliance officer appointed pursuant to subsection (3):-

(a) Access to any documents, records, registers and accounts necessary for the performance of his tasks,
(b) Power to request and obtain any information, notice, details or document from any employee of the reporting entity
(c) Other responsibilities as prescribed by the Regulator,
(d) Other functions necessary to implement the Act, rules, and directives.

1. Work as Focal Point to make the work as per directives to be effective.
2. Draft policy, procedure, systems to be made and presented to work as per act, ALPA rules in effective way.
3. To obtain information, report from Department/Branches officials, staffs about suspicious reporting and analysis.
4.. To have service from professional/specialist on this field, from department or officials, to have documents, details or information continuous manner any time.
5. To make report about the status of implementation of act and ALPA rules after doing inspection.

Bank shall establish separate Compliance Department and AML/CFT UNIT with **sufficient staffs and resources.**

Compliance Officer have to report for departmental action against officials and department not providing information, documents asked by compliance officer and bank has to take action against them and inform to **Board level AML CFT Committee.**

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..

Bank, while developing policy and procedure has made provision on combating financing in Terrorism activities and production of arms and ammunition. Further bank has AML software and procedural mechanism to identity, monitor and report about combating finance against terrorism.

To make implementation of this Act and Rules effective and result oriented, Bank shall provide following shareholders and, member of BOARD and higher management to participate in Organizational Capacity Development Program.

a Shareholder holding 2% or more shares in paid of capital, board of directors, higher management team, knowledge sharing programs on AML/CFT/KYC.

b.. For staff's regular interactive programs transferring knowledge on this subject.

c. Compliance Officer and staffs directly involved in AML/CFT Unit shall be sent for national and internal training, programs etc.

20. 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 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 risks which cannot be mitigated effectively

21. Prohibited customers and transactions:

Bank shall not do transactions with the followings:

1. Establish or maintain anonymous accounts, or accounts in fictitious names or transact in such accounts or cause to do so.
2. Maintain relationship with shell Banks or other banks which deals with shell bank or shell entities
3. 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. However, incase customer submits valid reason for inability of presenting some document or information and bank become satisfied with the reason, relationship can be established, and transaction can be done with maintaining record of the information of non-existence of document/information.
4. Customers who provide conflicting Documents, information and details.
5. Maintain relationship with the banks operating in offshore jurisdictions
6. Maintain relationship with persons and entities sanctioned by major sanction authorities such as United Nations, Office of Foreign Assets Control- United States, Her Majesty's Treasury-United Kingdom, 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. Use of accounts maintained by the bank for technical reasons, such as sundries accounts or transit account, or employees' accounts to filter or conceal customer transactions
10. Maintaining accounts under pseudonyms that are not readily identifiable
11. Opening Accounts without name or with notional name
12. Acceptances and documentation of collateral that do not corroborate with the actual economic situation or documentation of fictitious collateral for credit granted on trust
13. Payable through Accounts
14. Providing Downstream Correspondent Banking

15. Companies issuing bearer shares

16. Natural and legal person involved in producing and distributing illegal Arms and Ammunition

22. 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 decisions are the prime responsibility of the Bank's department/branch heads. Rigorous examination relating to the prospective customer's identity must be executed prior to opening any new account and processing a transaction.

i. While opening an account, the concerned staff should obtain all the required information as per viz. full name of the account holder, current address and place of work etc. as well as customer identification document as per NRB Directives verified with originals.

ii. Copy of Citizen Certificate/Voter ID/Passport

iii. All subsequent changes of information related to account holders shall be updated regularly. In case of a firm or a company the date of renewal of the firm/company shall always be recorded and tracked.

iv. The identification documents that are easily available in any name should not be accepted as the sole means of identification. Wherever the suspicion arises about the identity of the customer, the name and address should be further checked by one or more of the following means:

(a) Requesting sight of recent utility bill (e. g. water, electricity, telephone).
(b) A credit card (verify the current status).
(c) Existing Bank Account Statement.
(d) Tax identification / Returns.

v. It shall be the responsibility of the customers to notify the bank for materialistic changes, if any has taken place after the time of opening of account. Bank is not responsible for tracking the same however, bank shall update in regular KYC.

vi. prior to completion of opening of account, each customer's name is run through data filtration checking for any anomalies including sanctioned listing by local and/ or international agency.

23. Acceptable Identification Documents

The Bank shall obtain copy of identification documents of customers duly notarized / Certified by other Bank or Financial Institution / Government authorities or physically verified by authorized staff of the bank itself:

In case of Nepali citizen

i. Citizenship certificate/ Valid passport

ii. Additional documents for evidencing address in case of **difference in permanent and current address:** a. Voters ID b. Utility bills of electricity/water. c. Land ownership certificate. d. Certification from local authority. Driving License. e. Employee ID Card, (mandatory for Government employee/Government owned entity) f. ID of Nominee.

iii. National Identification Documents (NID).

iv. Certificate issued by District Administration Office, Metropolitan Office, Village Development Office identifying the person and his/her address with photograph.

v. In case of legal person or any other organization: Valid Certificate of Incorporation, Income Tax or PAN / VAT Registration, Certificate of Registration with District Administration Office or any other competent authority.

vi. Minimum document/certificate as specified by Central Bank of Nepal NRB from time to time must be obtained in all the cases.

vii. And any other documents specified in Customer Service Manual of the Bank.

viii. Extra documents, 2nd ID/EDD/Enhanced KYC is required for following customers to open accounts:

1. If customer is foreigner
2. If customer is from country not complying aml rules or if customer's main transaction is with such high-risk countries
3 If customer is listed in stock exchange of high-risk countries not fully compliant with AML rules.
4. If true beneficial owner is not clear.

5. If customer or true beneficial owner is PEP/PIP
6. If customer is suspicious or doubtful.
7. If Transactions is above Rs. 1 lac

Detail of the documents to be obtained while identifying customers shall be as per NRB Directives.

24. Categorization of Account Based on Inherent Risks (Risk categorization) (ALPA: 7N)

While opening account, customers shall be categorized for inherent risk like 'low' 'Medium' or 'High' and 'PEP' based on a criterion set. A periodical review of the accounts should be conducted to reassess the categorization.

Indicative list of risk categories has been illustrated in detail in Annexure **2 a**nd that of PEP/PIP **along with their family members and close associates** in Annexure 1 of this policy and also in Cash and Customer Manual of the Bank.

A. Low Risk: For the purpose of risk categorization, individuals and entities whose identity and source of wealth can be identified and transactions in their accounts by and large conform to the known profile may be categorized as low risk.

B. Medium Risk: Accounts not categorized in high risk and Low risk to be categorized in medium risk.

C. High Risk / PEP: All customer accounts with negative news, Global Watch list customer/ pep/pip and close family members to be included in high risk.

High net worth customers shall be defined by management from time to time.

The Bank shall pay special attention in the transaction of High-Risk account. All complex, unusual large transaction and all unusual patterns of transaction, business relationships and transactions relating to the customer and financial institution of a country internationally identified as a country that do not or insufficiently comply with AML/CTF international standards shall be monitored with special attention. Enhanced Customer Due Diligence should be conducted for the High Risk account and Copy of citizenship of the family members shall be obtained as specified in Customer KYC Form for Individual (Annex-in AML CFT Manual).

It is to be specifically noted that risk categorization is meant for proper monitoring of accounts and does not reflect in any way on the account holders. Risk Categorizations done by the Branch should not be disclosed to the customers**.** While the extent of knowledge / information available on customers to prove their identity sufficiently shall determine the risk perception and risk categorization.:

Branch should ensure that risk categorization of all customer accounts is completed expeditiously and thereafter reviewed at least once a year **for High Risk/PEP/PIP/High Networth Customers.**

25. Customer's Risk Profile

As a part of Customers' Risk Profile, 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

26. Certification of Documents

Concerned staff of Customer service department shall verify the documents submitted by customers with the original at the time of account opening. The staff should verify their copies against the original documents and affix his/her signature as confirmation of such verification.

A profile of customers' identity, social/financial status, nature of business activity and expected volume of transaction, turnover and the location of the customer address shall be prepared **in the form Customer ID in CBS.**

27. Monitoring Graded Accounts (Enhanced Customer Due Diligence) (EDD) (ALPA:7E)

The Compliance Officer at the branches must review the accounts regularly and submit reports to the Compliance Officer stationed at the Head Office. Branches shall follow appropriate measure of Enhanced CDD of the High risk categorized customer accounts and shall be reviewed on regular basis or as prescribed by the directives issued by NRB from time to time.

AML Software with the help of logics and alerts generated shall be used to monitor all sorts of accounts.

At the time of closing High Risk accounts, Branches to send the information to CICD -AML/CFT Unit through mail/memo about closure request. AML/CFT unit - CICD shall study/investigate the accounts in AML point of view before closing.

Branches shall be vigilant in case of frequent or large value movements of funds in any account irrespective of its category.

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 pursuant to section 35, 7D., 7U.
(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,
(f) High Networth customers
(g) Customer consuming high risk products and services,
(h) Customer suspected of ML, TF or other offense,
(i) Other customers as prescribed by the Regulator.

While establishing commercial transactions with the above customer, EDD shall be obtained for following customers also.

a. Transactions done through electronic medium which is systematical unusual and suspicious in nature
b. High net worth customers
c. Customers who can be involved in money laundering and financial crime.
d. Countries put in high risk due to Corruption, tax evasion and other criminal grounds **and as defined by FATF as HR.**
e. Heavy cash related business, gold business, petrol pumps, department store chain store etc. or customer using new technology or systems.
f. Person who is convicted by court under unethical crimes as per the prevailing law.
g. Identification of Source and verification of the same and outcome of investigation to be on record and to be provided on demand.
h. Possible way out to find out Grounds of transactions of customer and purpose
i. Identification of unusual and suspicious transaction/customer
j. Additional details about beneficial owner
k.. Details of nature of transactions, purpose of the transactions and additional detail if required to be asked.
l. Approval from top management whether to continue or not continue the transaction relation with the customers, **based on case to case basis.**
m. To fix the threshold, **if required.**
n. To obtain source of funds and deposits.
o. Source of transactions and documents verification.
p. Information about purpose of transactions and documentary proof of the same.

Following additional steps shall be taken besides above.

a . Source of assets/funds
b. Purpose of transactions.
c. To fix the threshold to monitor the transactions.

Copy of **Citizenship certificate of close** relatives of customers who falls in EDD process including pep/pip/High risk to be obtained **as far as possible.**

KYC Officers of Concerned Branch shall review the accounts of high-risk customers/high net worth customers and update ECDD **at least once in a year.**

28. Detection of Other Possible Money Laundering Transactions (Walk-In Customer/ Non-Account base customer)

For any non account holders, Branch shall carefully and systematically verify and obtain copy of identity of the customer with contact no in all cases. In this context, the identification process normally entails obtaining customer details such as name and full address, physical verification of customer's original identification document, Copy of such ID signed by the customer should be retained with the authentication by the concerned staff involved in processing the transaction with contact no.

29. Wire /Electronic transfer (ALPA: 7 L)

Staff of Remittance Department 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, the ordering bank/ FI shall include full information of the Originator and Receiver to process the payment as mentioned in above.
i. On request by FIU or Paying Institution, the details of the originator shall be provided latest by three working days in Domestic Electronics Transfer.
j. 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.
k. Unscheduled group transaction that increases risk of money laundering and terrorist funding should not be allowed.

Bank, prior to initiating wire transfer/ Swift Transfer, has to run down data filtration process to check if individual/ entities involves in transfer/ recipients are subject to sanctioned list/ or categorization for PEP, to rate the transactions and seek additional documents/ information to best satisfaction after verifying with data base through Swift Sanctions screening.

It shall be the responsibility of concerned staff initialing this transaction to screen the applicant/beneficiary and other related parties, if any, with the help of KYC officer through Screening Software (Presently Acuity ASM.

Banks use wire transfers as an expeditious method for transferring funds between bank accounts.

branches must ensure that all wire transfers are accompanied by the following information:

(A) In Cross-Border Wire Transfers

a) All cross-border wire transfers must be accompanied by accurate and meaningful originator information.

1. If required information not disclosed and felt suspicious, bank can deny sending such transfer and report to the concerned.
2. Bank shall make data base of wire transfer done about individual and organization and if any

organization or individual wire transfer **that does not match with the profile and nature of business** should be informed/**reported** to FIU

b) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included. It should further include name and account number (where account number is not available unique reference number for identification of transaction) of the beneficial owner.

c) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (b) above.

(B) In Domestic Wire Transfers

a) Information accompanying all domestic wire transfers must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means. It should further include name and account number (where account number is not available unique reference number for identification of transaction) of the beneficial owner.

b) If a bank has reason to believe that a customer is intentionally structuring wire transfers to below threshold to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on **completing** customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be submitted to FIU.

c) When a credit or debit card is used to effect money transfer, necessary information as (a) above should be included in the message.

Exemptions

Inter-bank transfers and settlements, where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

Role of Ordering, Intermediary and Beneficiary

(a) Ordering Bank

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. The ordering bank must ensure that qualifying wire transfers contain complete originator information. The bank must also verify and preserve the information at least for a period of ten years.

(b) Intermediary Bank

For both cross-border and domestic wire transfers, a bank processing an intermediary element of a chain of wire transfers must ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept at least for ten years by the receiving intermediary bank of all the information received from the ordering bank.

(c) Beneficiary Bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should

be reported to the Financial Information Unit. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

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.

30. Terrorism Financing

i. In terms of Section 80 of the Banks and Financial Institutions Act, 2063 Nepal Rastra Bank directs banks from time to time to freeze any account opened in the concerned licensed institution in the name of any individual, firm, company or institution in such a manner as to prevent the withdrawal or transfer of funds in any way from that account in connection with investigations into any type of crime or in connection with protecting the national interests by checking national or international terrorist activities or organized crimes. To ensure compliance of NRB instruction regarding freezing of accounts as aforesaid CCD, Corporate Office shall develop necessary system to:

a. Maintain updated designated lists in electronic form and run a check on the given parameters on a 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 .

b. In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the Branches/Offices shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the forms of bank accounts, held by such customer on their books to the Compliance Officer, Corporate Office. The Compliance Officer then immediately passes the information to FIU. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

c. In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the branches would prevent designated persons from conducting financial transactions, under intimation to Compliance Officer, Corporate Office. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

d. The Branches shall also send a Suspicious Transaction Report(STR) with the Compliance Officer, Corporate Office covering all transactions in the accounts covered by paragraph (b) above, carried through or attempted, as per the prescribed format. It shall be the duty of the compliance Officer, AML/CFT Unit, corporate office to arrange analyze and investigate on the STR received from the Branches and immediately file Suspicious Transaction Report (STR) with the FIU in the prescribed format if he/she deems that the STR received from the Branches needs to be reported to FIU as a STR.

(ii) Freezing of financial Assets

a. Nepal Rastra Bank may request 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 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.

(iii) Procedures for Unfreezing of funds, Financial Assets or economic resources or related services of Individuals/Entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person.

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned Branch. The Branches shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the AML/CFT Unit- Compliance Officer, Corporate Office within two working .

The Compliance Officer shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, puts up a note to the Head CICD who then shall pass an order within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned branch.

However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, CICD shall inform the applicant through the concerned Branch.

(iv) Screening of Customers and related individual/entities before establishing relationships (Customer On-boarding) shall be as per AML CFT Manual.

31. Trade based Money Laundering:

Proper screening is done at the time of approval of facilities as well as at the time of sending the payment against Sanctioned list/ PEP/PIP of applicant as well as beneficiary.
Document to be checked whether the shipment is form 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.

Transactions and business pattern shall be monitored closely by concerned Relationship managers/TOC to identify possible TBML and if any suspicious nature of transactions or business activities are noticed, the concerned RM must send STR to AML CFT/CICD immediately in a prescribed format.

32. Re-submission Policy/Rejections Cases:

a. Trade: Trade department to properly keep record of changes made in port of shipment, change in shipping company, beneficiary details, or country that is in sanctioned list.
Keep track of re-submission request if any and report to CICD for proper action to be initiated.

b. Credit: Separate Record of re-submission/rejections cases to be kept. Reason for rejected cases to be referred to concerned department at Head Office and CICD and to be kept in Knowledgebase which shall be refered by all concerned.

c. Operation: Re-submission cases related to operations should be maintained. Account opening rejected due to reasons related to AML/CFT should be recorded and referred to CICD through mail. CICD will keep in knowledge base to be referred by all concerned.

33. Money Laundering in Credit:

Use of funds taken as loan can also be misused for money laundering purpose. Loan of PEP/PIP to be approved by Senior Management even if it is within authority of concerned Branch Manager/In charge.

Branch Managers and Relationship managers shall monitor the intended use of credit facilities by the customer and shall report immediately if any deviation is noticed on the intended use of loan.

For transaction monitoring purpose, concerned relationship mangers shall monitor the transactions of credit customers and initiate to submit STR to Head Office if any suspicious transactions/activities are noticed.

34. 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.**

35. 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.

36. Complete Record Keeping (ALPA:7R)

All the documents and records as mentioned below shall be maintained accurately and securely for minimum Five years after the termination of business relationship or from the date of transaction in case of occasional transaction.

1. All documents and other information related to the identification and verification of customer and beneficial owner.
2. All documents, records and conclusion of the analysis of customer or beneficial owner and transaction, Customer identification document should be held in all customer files. It is the responsibility of Customer Service Department of the Branch to ensure this
3. Customer identification and transaction documents should be retained for at least 5 years after closure of the account/transaction.
4. Documents and details of account and business relation
5. All documents and records relating to domestic and foreign transactions,
6. Records of **monitoring of** all suspicions **transactions** and reports to the Financial Information Unit and/or other concerned authority shall be safely maintained for **Five Years.**
7. Other documents and records as prescribed by regulators.
8. Records of all training related to ML and TF provided to staff shall be maintained. It shall also include nature and name of staff attending the training.

As far as possible, such records are maintained in digital form as well.

37. Awareness and Training On AML/CFT

All staffs shall be aware of the statutory and regulatory obligations. Therefore, **Human Resource Department in coordination with** the Designated Compliance Officer at Head Office or person assigned by Compliance Officer at Head Office shall be responsible for conducting employee training program in Coordination with on ongoing basis, so that all related staffs are adequately trained on the AML/KYC and CDD policies/procedures. The training requirements may be different for the front-line staff, compliance staff and staff dealing with new customers. However, initial training should be provided to all staff with regard to money laundering and Terrorist financing activities and means to control/ counter them. Staff shall be regularly updated upon any change of responsibilities.

Training outside valley and inside valley shall be conducted time and again in coordination with HR and as far as possible with Central Operations. Training on AML/CFT/KYC issues is Mandatory every year for all front line and operations related staffs. Training shall include other employees of the banks.

The training shall be focused on providing the risk-based training, explanation to the latest regulatory guidelines, corporate governance, KYC, money laundering issues etc. in coordination with Human Resource and Central Operation, audio visual, latest directives form Central Bank

Effective discussion with the participants shall be done and take their queries. Training assessment with respect to AML CFT to map the understanding of participants shall also be done.

Banks' concerned staffs shall be sent for training on AML/CFT on national as well as international level.

Shareholder holding shares above 2%, BOD and senior management shall also participate in AML/Training every year.

Human Resource Department (in coordination with AML CFT Unit/CICD) shall arrange knowledge sharing program on latest developments on the subject.

Remittance **Principal Agents** shall conduct AML CFT Training to their staff and sub agents in an annual basis and compliance of the same is monitored by Compliance/AML CFT Unit.

Soon after recruitment, Induction Training on AML/CFT issues shall be carried out compulsorily by HRD

38. Risk Assessment and Risk Management (RM) (ALPA:7D)

Risk Assessment and Risk management:

(1) Bank shall identify and assess risks on ML and TF in accordance with its business or profession, scope, customer, products or services, geography, sectors, transactions or delivery channel etc.

(2) Bank, while conducting risk assessment pursuant to sub-section (1), shall also consider the findings of the national and regulatory risk assessment.

(3) Bank shall, while conducting risk assessment pursuant to sub-section (1), determine the level of risks by analyzing all relevant risk factors.

(4 Bank shall maintain records of conclusion of risk assessment and all related details and information.

(5) Bank shall conduct and update the risk assessment pursuant to subsection (1) periodically or as per necessity.

(6) Bank shall make available to the Regulator any risk assessment undertaken pursuant to subsection (4), and also make it available to other concerned agency upon demand.

(7) Bank shall undertake customer due diligence measures in accordance with the level of risks as identified pursuant to this section and shall establish appropriate policy, procedural and risk management measures, to manage and mitigate such risks and update such measures.

(8) Bank regularly monitor the execution of policy, procedural and risk management measures pursuant to sub-section (7) to ascertain whether they are in implementation or not.

Following additional grounds are also considered while doing risk assessment management of customers

A. Based on Geographical locations and regional risk assessment. – National Risk Assessment report.

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

C. Commercial relations, threshold transactions and nature.

(9) **AML CFT Risk Assessment is done periodically as directed by NRB** and necessary update on the policy and procedural manual shall be done accordingly. A copy of **Risk Assessment** report shall be sent to NRB as per requirement.

(10) 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.

(11) 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 of the bank.

39. Non-compliance with Bank's AML/CFT/ KYC Policy and procedures

Any staff failing to abide by the policy and procedures set by the Bank to prevent money laundering and terrorist financing 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.

40. Regulatory Obligations (ALPA: 7V)

The Bank would be obligated to comply with the requirements of the AML/ CFT law and with the relevant provision of the Banking Act. It is a regulatory offense for an institution not to have in place procedure to combat money laundering and terrorist financing. The procedures include, customer identification,

customer verification, Know your customer, Reporting threshold transaction, Recognition and reporting suspicious transaction, record keeping and training of staff.

Department of Money laundering Investigation and Regulator deals AML/ CFT violation and violators strictly. Any one or all of the following actions or sanctions against a financial entity failing to comply with any provisions of the ML prevention (Second amendment) Act 2013, Rules or Directives issued there under or order may be imposed-

i. To impose fines from Rs..one million to Fifty million on the basis of gravity of violation of the Act, rules or order or directives,
ii. To impose full or partial restriction on the business, profession or transaction
iii. To suspend the registration or permission or license,
iv. To revoke the permission or license or cancel the registration,

The regulator may impose other appropriate sanctions under prevailing laws if the sanctions provided are not enough for the violation of the provisions of ALPA.

41. 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, false accounting - falsification or alteration of accounting records or other documents- 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.

c. Identifying fraud and money laundering:
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 and money laundering prevention and detection.

All staff, irrespective of grade, position or length of service have to be appropriately trained on an on-going basis in order to be able to work towards preventing and detecting fraud and money laundering. Fraud, and money laundering prevention and detection matters shall be included in the Bank's induction programs and continuous career training.

d. Fraud and money laundering reporting and investigation.

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

Any suspicions of fraud, or money laundering Red Flags activities noted/observed should be reported to Central Operation/HRD/Compliance and Internal Control Department

PART C – ROLES AND RESPONSIBILITIES

1. Roles and Responsibilities of Board

1.1. 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:

1.2 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

1.3 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.

1.4 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 related to AML/CFT at least on quarterly basis and furnish the review report on the implementation of the directives to FIU on half yearly basis.

1.5. The Board of Directors of the bank and financial institutions 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.

1.6 The Board of Directors of the Bank shall effectively discharge its statutory responsibilities as elaborated herein above.

1.7 The Board is authorized to issue appropriate instructions to the senior management regarding Investment Policy that it deems appropriate.

1.8 Any amendments / cancellation or revision in this policy shall be at the sole discretion of the Board.

2. Roles and responsibilities of Risk Management Committee (RMC)

2.1 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.

2.2 The committee shall conduct policy level analysis for credit, market and operation risk management and update, monitor and recommend suitable measures to the BOD.

2.3 Ensure that adequate controls and systems are in place to identify and address **AML CFT** and operational risk.

2.4 Assess the quality and appropriateness of mitigation action.

3. Roles and Responsibility of Operation Risk Management Committee

3.1 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.

3.2 To clearly assign authority, responsibility and reporting relationships and ensure that necessary resources are available to manage operational risk effectively.

3.3 To discuss on policies procedure related to operations AML/CFT/KYC issues **raised** from Compliance /AML/CFT unit.

3.4 To develop mechanism to minimize risk related to operational issues on AML/CFT/KYC issues.

3.5 To discuss on branch inspection report on operation risk/lapses and discuss on signals/breaches on occurrence of probable risk associated.

3.6 To discuss on the issues pointed out by Auditors related to operations.

3.7 To work for introducing controls wherever required.

4. 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-

4.1 **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.**

4.2 To discuss on sufficiency of Policyl 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.

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

5.1 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:

5.2 Circulate and implementation of the Policy approved by the Board.

5.3 Carry out and manage the Bank's activities in a manner consistent with the business strategy, risk appetite and other guideline provided by the board.

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

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

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

5.7 CEO shall also ensure that enough resources and required access to information, documents and staffs.

5.9 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 month from the end of fiscal year.

5.10 Other discretionary authorities shall be exercised as delegated in the Policy or by the Board from time to time.

5.11 The bank's senior management shall be responsible for identifying and managing the compliance risk through all levels of the organization. Whenever breaches are identified senior management will take appropriate remedial or disciplinary action. With the assistance of the CICD/AML-CFT Unit Senior Management shall assess the main compliance risk issues facing the bank and the plans to manage them.

6. Role and Responsibilities of Executive Operating Officer (EOO)

6.1 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. The illustrative but not exhaustive roles and responsibilities of Executive Operating Officer of the Bank related to this Policy are as follows:

6.2 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 through the Branches.

7. Roles and Responsibilities of Departments

7.1 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.

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

8. Roles and Responsibilities of Branch Managers

8.1 To ensure all regulatory instructions are complied it.

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

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

8.4 Supervise day to day operational function of the branch including vault and ATM Balancing.

8.5 Be Knowledgeable about all deposit/business and loan products.

8.9 Supervise and develop staff regarding service expectations, policies/procedure/products/system and banking transaction.

8.10 Various other responsibilities as mentioned in job description.

9. Roles and Responsibilities of Operation In-charges /Operation Managers (at Branch Level)

9.1 Operation Managers/in charges shall be responsible for ensuring proper implementation of control, and monitoring and reporting procedure across the branch under their control to prevent ML/TF.

10. Roles and Responsibilities of staff in Customer Services Departments (at Branch Level)

10.1 Customer identification and acceptance process to be followed as directed.

10.2 Proper risk categorization as per instruction from management and as per policy.

10.3 Not to open prohibited accounts as highlighted in the policy.

10.4 CDD/EDD to be done as directed

10.5 Necessary screening before un boarding customers.

10.6. Various other job as per job description provided**.**

11. Roles and Responsibilities of Compliance Officers/KYC Officers (at Branch Level and Head Office)

11.1 KYC and 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.

11.2 They shall be primarily responsible for monitoring high value and high-risk transactions, detecting suspicious activities and report suspicious transactions/activity to AML Implementing Officer of the Bank.

11.3 The roles and responsibilities of the Branch AML Implementing officers shall be covered in their job description. Any other responsibility as decided by Board and Risk Management Committee/AML/CFT Committee.

12. 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:

12.1 Internal Audit shall provide independent evaluation of compliance with this policy.

12.2 Internal Auditor shall be responsible for conducting checks and reviews to ensure that the control and monitoring and reporting procedures under this policy.

12.3 Internal audit shall specifically check and verify the application of KYC/AML/CFT procedures at the offices/branches and comment on the lapses observed.

12.4 The compliance in this regard shall be placed on the Audit committee and the board

12.5 Ensure the process and procedures mentioned in this Policy are duly followed.

12.6 Check the breach of internal and external provision and regulations.

12.7 Conduct the audit as per the provision of NRB.

13. Role and Responsibilities of Human Resource Department

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:

13.1 HR Department 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.

13.2 HR shall also ensure that due diligence of the employees is updated regularly, and record is maintained appropriately.

13.3 Assessment of adequate human resources requirement.

13.4 Training to human resources in the area of AML / CFT on **regular** basis **as per regulatory requirement**.

14. Roles and Responsibilities of Individual Employees

14.1 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.

14.2 Any staffs 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 following standard procedure framed under this policy and shall be mandatory role of all staffs of the bank.

15. Roles and Responsibilities of Compliance Officer /Head office:

15.1 To manage and implement the AML CFT KYC issues as directed by concerned regulatory body through AML/CFT Unit under Compliance.

15.2 To perform duties and responsibilities related to AML/CFT/KYC as highlighted in respective Job Descriptions.

15.2 To work as per TOR of the Compliance and Internal Control Department

16. 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

17. Roles and Responsibilities of Reporting Cell

17.1 Compile, check and send the report to central bank regulatory concerns as per the guidelines and requirement, **based on this policy as well.**

17.2 Provide various reports to senior management and department as and when required.

17.3 Update to senior management MIS on daily basis.

18. Roles and Responsibilities of Legal Department

18.1 Legal Department is the department responsible for keeping eyes on legal compliance of the Banking operation.

18.2. Providing legal opinion as and when required.

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

19. Roles and Responsibilities of Province Heads and Provincial 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.

Other various roles and responsibilities of different Authorities, Committees, Executives, Departments and Employees shall be as outlined in their respective job descriptions/TOR.

Part D: ANNEXURE

ANNEXURE 1: INDICATIVE LIST OF PEP/PIP, FAMILY MEMBERS AND CLOSE ASSOCIATES

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

1.1. Administrators/Politicians

- President, Vice Presidents
- Prime Minister and Incumbent ministers
- Advisors of Prime Minister
- 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 and Sub Municipalities (if they are in Key positions of political parties e.g Central Committee Members or relatives of such members).
- Chairman and Vice Chairman of District Coordination Committees **and Rural Municipalities**
- Chief Election Commissioner and all Commissioners of Election Commission
- Auditor General
- Attorney General
- Chief and all members 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

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

- Additional Inspector General of Police and above

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

- Chairman
- Chief Executive Officers

1.6. CEO/Chairman of Public Enterprises.

2. Immediate Family Members of PEP/PIP

- Parents,
- Siblings unmarried
- Spouse,
- Children,
- In-laws for married woman
- Grandparents and grandchildren.

3. 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.

ANNEXURE 2: INDICATIVE LIST FOR RISK CATEGORIZATION

1. Low Risk

For the purpose of risk categorization, individuals and entities whose identity and source of wealth can be identified and transactions in their accounts by and large conform to the known profile and the volume does not breach our threshold of Rs. 1 million may be categorized as low risk. Followings are the indicative list of Low Risk customers:

- Public sector enterprise fully owned by Government of Nepal or their fully/majority owned subsidiary.
- Government Departments, Regulators, Statutory Bodies etc.
- Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken.
- Pensioners, benefit recipients, persons whose income is from their partner's employment (e.g house wife, students)
- Financial Institutions enlisted in the Security Exchange Board.
- Salaried employees whose salary structures are well defined.
- Personal account having balance up to Rs. 5 00,000.
- People belonging to lower economic group of society whose accounts show small balances and minimal turnover.
- Self employed individuals.
- Local resident(s).
- Public limited company and its subsidiary.
- Borrowing customer which does not rely mainly on cash source
- International Charities and Non Government Organizations that are operating for over 10 years with transparent working area and not receiving donations from abroad.
- customers other than those classified as High or Medium Risk

2. High Risk

Known customers that are likely to pose a higher risk to Banks and Financial Institutions should be categorized as "High Risk" depending on the customers' background, nature and location of activity, sources of funds, etc. Compliance Officer should apply enhanced due diligence measures based on the risk assessment for high risk customers, especially those for whom the sources of funds are not clear. Following are the indicative list of customers that can be categorized as High Risk:

- Person/outlet dealing with gambling, money exchange, jewelry, land broker, dealers in high value commodities
- Non-Financial Institution that carry financial transactions (Money Transmitters)
- Financial intermediaries
- Cash intensive/oriented business (such as tolls, gaming companies, casinos etc.)
- Antique Dealers, Money Service Bureau and Dealers in arms.
- Customers who may appear to be Multi Level Marketing companies.
- Accounts of bullion traders i.e. gold/silver/diamond and gems/jewelers.
- Politically Exposed Person or People in Influencing Positions (mentioned in Annex – 1)
- Family members and close associated (as per Annex 1) of PEP/PIP
- High net worth individuals as defined by Bank Management
- Other group of person like Notaries, Lawyers and Chartered Accountants as designated by the Government of Nepal upon the recommendation of National Coordination Committee.
- Trusts, charities, NGOs and organizations receiving donations from abroad (other than those promoted by UN or its Agencies)
- Companies having close family shareholding or beneficial ownership
- Firms with Sleeping Partners
- Client accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc.
- Customers based in high risk countries/jurisdictions and countries identified by FATF as having strategic deficiencies in compliance of AMLCFT standards.
- Investment Management/Money Management and or personal investment company
- Individuals and entities specifically identified by Regulators, FIU and other competent authorities as 'High Risk'.
- Individuals with dubious reputation as per available public information
- Customers who provide insufficient or suspicious information
- Customer with whom the Bank or its agent have not had any face to face meeting.
- Non Resident (Foreign National) Customers
- Citizen who have transactions with the countries who are on high risk with respect to AML
- If Beneficial owner not clear
- **If Beneficial owner is PEP/HR and holds more than 50% shares.**
- **Joint account if any of the customer is categorized as HR.**

- Travel Agencies
- Vehicle Sellers
- **Embassy/Consulate**
- **High Net-worth Customers (for one year if net-worth is low since one year)**
- All customers that do not fall in either in low or medium Risks

3. Medium Risk

- Non Banking Finance Companies(e.g. Insurance companies, cooperatives etc.)
- Builders
- Stock Brokers
- 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 except those as categorized as HR.
- All customers that do not fall in either in Low or High Risks
- **Indian Nationals with balance less than Rs. 1M with turnover less that 1RsM in a quarter. (For this purpose, Central operations shall monitor quarterly the balance and turnover and change the Risk category accordingly)**
- **Foreign Nationals (Except from FATF high risk countries) with balance less than Rs. 0.1M with turnover less that Rs. 1M in a quarter. (For this purpose, Central operations shall monitor quarterly the balance and turnover and change the Risk category accordingly)**

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 (FATF)

▪ 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 a 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**

v. Purchase or sale of large amounts of precious metals by an interim customer.
vi. Purchase of bank cheques on a large scale by an interim customer.
vii. Extensive or increased use of safe deposit lockers, which do not appear to be justified by the customer's personal or business activities.
viii. Cash payments remitted to a single account by a large number of different persons.
ix. 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,
x. 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.

ANNEXURE 4: AML CDD REVIEW QUESTIONNAIRE FOR CORRESPONDENCE BANKS/FIS/VOSTRO PARTNERS

HBL- AML Questionnaire based on Wolfsberg Group Financial Crime Compliance Questionnaire (FCCQ) v1.0

Financial Institution Name:			
Location (Country) :			
No #	**Question**		**Answer**
1. ENTITY & OWNERSHIP			
1	Full Legal Name		
2	Append a list of branches which are covered by this questionnaire		
3	Full Legal (Registered) Address		
4	Full Primary Business Address (if different from above)		
5	Date of Entity incorporation / establishment		
6	Select type of ownership and append an ownership chart if available		
6 a	Publicly Traded (25% of shares publicly traded)		Y N
6 a1	If Y, indicate the exchange traded on and ticker symbol		
6 b	Member Owned / Mutual		Y N
6 c	Government or State Owned by 25% or more		Y N
6 d	Privately Owned		Y N
6 d 1	If Y, provide details of shareholders or ultimate beneficial owners with a holding of 10% or more		
7	%of the Entity's total shares composed of bearer shares		
8	Does the Entity, or any of its branches, operate under an Offshore Banking License (OBL) ?		Y N
8 a	If Y, provide the name of the relevant branch/es which operate under an OBL		
2. AML, CTF & SANCTIONS PROGRAMME			
9	Does the Entity have a programme that sets minimum AML, CTF and Sanctions standards regarding the following components:		Y N
9 a	Appointed Compliance Officer with sufficient experience /expertise		Y N
9 b	Cash Reporting		Y N
9 c	CDD		Y N
9 d	EDD		Y N
9 e	Beneficial Ownership		Y N
9 f	Independent Testing		Y N
9 g	Periodic Review		Y N
9 h	Policies and Procedures		Y N
9 i	Risk Assessment		Y N
9 j	Sanctions		Y N
9 k	PEP Screening		Y N
9 l	Adverse Information Screening		Y N
9 m	Suspicious Activity Reporting		Y N
9 n	Training and Education[1]		Y N
9 o	Transaction Monitoring		Y N
10	Is the Entity's AML, CTF & Sanctions policy approved at least annually by the board or equivalent Senior Management Committee?		Y N
11	Does the Entity use third parties to carry out any components of its AML, CTF & Sanctions programme?		Y N
11a	If Y, provide further details		
3. ANTI BRIBERY & CORRUPTION			
12	Has the Entity documented policies and procedures consistent with applicable ABC regulations and requirements to [reasonably] prevent, detect and report bribery and corruption?		Y N
13	Does the Entity's internal audit function or other independent third party cover ABC Policies and Procedures?		Y N
14	Does the Entity provide mandatory ABC training to:		Y N
14 a	Board and Senior Committee Management		Y N
14 b	1st Line of Defence		Y N
14 c	2nd Line of Defence		Y N
14 d	3rd Line of Defence		Y N
14 e	3rd parties to which specific compliance activities subject to ABC risk have been outsourced		Y N
14 f	Non-employed workers as appropriate (contractors / consultants)		Y N
4. POLICIES & PROCEDURES			
15	Has the Entity documented policies and procedures consistent with applicable AML, CTF & Sanctions regulations and requirements to reasonably prevent, detect and report:		
15 a	Money laundering		Y N
15 b	Terrorist financing		Y N
15 c	Sanctions violations		Y N
16	Does the Entity have policies and procedures that:		
16 a	Prohibit the opening and keeping of anonymous and fictitious named accounts		Y N
16 b	Prohibit the opening and keeping of accounts for unlicensed banks and / or NBFIs		Y N
16 c	Prohibit dealing with other entities that provide banking services to unlicensed banks		Y N
16 d	Prohibit accounts / relationships with shell banks		Y N

1

16 e	Prohibit dealing with another Entity that provides services to shell banks	Y	N
16 f	Prohibit opening and keeping of accounts for Section 311 designated entities	Y	N
16 g	Prohibit opening and keeping of accounts for any of unlicensed / unregulated remittance agents, exchanges houses, casa de cambio, bureaux de change or money transfer agents	Y	N
16 h	Assess risks of relationships with PEPs, including their family and close associates	Y	N
16 i	Define escalation processes for financial crime risk issues	Y	N
16 j	Specify how potentially suspicious activity identified by employees is to be escalated and investigated	Y	N
16 k	Outline the processes regarding screening for sanctions, PEPs and negative media	Y	N
17	Has the Entity defined a risk tolerance statement or similar document which defines a risk boundary around their business?	Y	N
18	Does the Entity have record retention procedures that comply with applicable laws?	Y	N
18 a	If Y, what is the retention period?	_Years	

5. KYC, CDD and EDD

19	Does the Entity verify the identity of the customer?	Y	N
20	Do the Entity's policies and procedures set out when CDD must be completed, e.g. at the time of onboarding or within 30 days	Y	N
21	Which of the following does the Entity gather and retain when conducting CDD? Select all that apply:		
21 a	Ownership structure	Y	N
21 b	Customer identification	Y	N
21 c	Expected activity	Y	N
21 d	Nature of business / employment	Y	N
21 e	Product usage	Y	N
21 f	Purpose and nature of relationship	Y	N
21 g	Source of funds	Y	N
21 h	Source of wealth	Y	N
22:	Are each of the following identified	Y	N
22 a	Ultimate beneficial ownership	Y	N
22 a1	Are ultimate beneficial owners verified?	Y	N
22 b	Authorised signatories (where applicable)	Y	N
22 c	Key controllers	Y	N
22 d	Other relevant parties	Y	N
23	Does the due diligence process result in customers receiving a risk classification?	Y	N
24	Does the Entity have a risk based approach to screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	Y	N
25	Does the Entity have policies, procedures and processes to review and escalate potential matches from screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	Y	N
26	Does the Entity have a process to review and update customer information based on:	Y	N
26 a	KYC renewal	Y	N
26 b	Trigger event	Y	N
27	From the list below, which categories of customers or industries are subject to EDD and / or are restricted, or prohibited by the Entity's FCC programme?	Y	N
27 a	Non-account customers	Y	N
27 b	Offshore customers	Y	N
27 c	Shell banks	Y	N
27 d	MVTS/ MSB customers	Y	N
27 e	PEPs	Y	N
27 f	PEP Related	Y	N
27 g	PEP Close Associate	Y	N
27 h	Correspondent Banks	Y	N
27 h1	If EDD or EDD & Restricted, does the EDD assessment contain the elements as set out in the Wolfsberg Correspondent Banking Principles 2014?	Y	N
27 i	Arms, defense, military	Y	N
27 j	Atomic power	Y	N
27 k	Extractive industries	Y	N
27 l	Precious metals and stones	Y	N
27 m	Unregulated charities	Y	N
27 n	Regulated charities	Y	N
27 o	Red light business / Adult entertainment	Y	N
27 p	Non-Government Organisations	Y	N
27 q	Virtual currencies	Y	N
27 r	Marijuana	Y	N
27 s	Embassies / Consulates	Y	N
27 t	Gambling	Y	N
27 u	Payment Service Provider	Y	N
27 v	Other (specify)	Y	N
28	If restricted, provide details of the restriction	Y	N

6. MONITORING & REPORTING

29	Does the Entity have risk based policies, procedures and monitoring processes for the identification and reporting of suspicious activity?	Y	N
30	What is the method used by the Entity to monitor transactions for suspicious activities?	Y	N
30 a	Automated	Y	N
30 b	Manual	Y	N
30 c	Combination of automated and manual	Y	N

31	Does the Entity have regulatory requirements to report currency transactions?	Y	N
31 a	If Y, does the Entity have policies, procedures and processes to comply with currency reporting requirements?	Y	N
32	Does the Entity have policies, procedures and processes to review and escalate matters arising from the monitoring of customer transactions and activity?	Y	N

7. PAYMENT TRANSPARENCY

33	Does the Entity adhere to the Wolfsberg Group Payment Transparency Standards?	Y	N
34	Does the Entity have policies, procedures and processes to [reasonably] comply with and have controls in place to ensure compliance with:	Y	N
34 a	FATF Recommendation 16	Y	N
34 b	Local Regulations	Y	N
34 b1	Specify the regulation	Y	N
34 c	If N, explain		

8. SANCTIONS

35	Does the Entity have policies, procedures or other controls reasonably designed to prohibit and / or detect actions taken to evade applicable sanctions rohibitions, such as stripping, or the resubmission and / or masking, of sanctions relevant information in cross border transactions?	Y	N
36	Does the Entity screen its customers, including beneficial ownership information collected by the Entity, during on boarding and regularly thereafter against Sanctions Lists?	Y	N
37	Select the Sanctions Lists used by the Entity in its sanctions screening processes:	Y	N
37 a	Consolidated United Nations Security Council Sanctions List (UN)	Y	N
37 b	United States Department of the Treasury's Office of Foreign Assets Control (OFAC)	Y	N
37 c	Office of Financial Sanctions Implementation HMT (OFSI)	Y	N
37 d	European Union Consolidated List (EU)	Y	N
37 e	Other (specify)	Y	N
38	Does the Entity have a physical presence, e.g., branches, subsidiaries, or representative offices located in countries / regions against which UN, OFAC, OFSI, EU and G7 member countries have enacted comprehensive jurisdiction-based Sanctions?	Y	N

9. TRAINING & EDUCATION

39	Does the Entity provide mandatory training, which includes:	Y	N
39 a	Identification and reporting of transactions to government authorities	Y	N
39 b	Examples of different forms of money laundering, terrorist financing and sanctions violations relevant for the types of products and services offered	Y	N
39 c	Internal policies for controlling money laundering, terrorist financing and sanctions violations	Y	N
39 d	New issues that occur in the market, e.g., significant regulatory actions or new regulations	Y	N
40	Is the above mandatory training provided to :		
40 a	Board and Senior Committee Management	Y	N
40 b	1st Line of Defence	Y	N
40 c	2nd Line of Defence	Y	N
40 d	3rd Line of Defence	Y	N
40 e	3rd parties to which specific FCC activities have been outsourced	Y	N
40 f	Non-employed workers (contractors /consultants)	Y	N

10. AUDIT

41	In addition to inspections by the government supervisors / regulators, does the Entity have an internal audit function, a testing function or other independent third party, or both, that assesses FCC AML, CTF and Sanctions policies and practices on a regular basis?	Y	N

11. DOCUMENT REQUIREMENT

Please provide us the copies of the documents as listed below

A	License(s)	
B	Article of Association	
C	Memorandum of Association	
D	AML/Compliance Policy	
E	Share holding pattern	
F	Organizational Chart	
G	List of Board of Directors and Senior management with their ID copy and current residential address	
H	Most recent Audit Report	

12. DECLARATION

I hereby declare that, to the best of my knowledge, the above information is correct, accurate and reflective of my company's anti money laundering, combating terrorism financing and sanctions compliance policies, procedures and programs.

On request of Himalayan Bank Limited, we will furnish the details and particulars of enhanced due diligence performed on the transaction routed through Himalayan Bank Limited.

Authorized signature	
Name:	
Designation:	
Tel No. & Cell No.	
E-mail address	
Date:	
Company seal	

ANNEXURE 5: AML/CDD REVIEW QUESTIONNAIRE FOR PRINCIPAL AGENTS

HBL हिमालयन बैंक लिमिटेड Himalayan Bank Ltd.

'A' Class Licensed Financial Institution

Anti Money Laundering & Know Your Customer Questionnaire

PART 1: GENERAL INFORMATION	
CONTACT DETAILS	
Full Legal Name of Institution	
Registered Address	
Please list any name abbreviations this company also uses:	
Address of Head Office	
E-mail	
Website (if any)	
No. of Employees	
Indicate all financial products and services offered by your institution:	
List all other remittance service with whom your institution currently has/had, a business relationship with.	
Has the institution ever been restricted, suspended, or terminated by another money remitter service provider?	☐ Yes ☐ No
Please provide the list of your Top Ten (10) agents in terms of Volume of Transactions in last FY	
REGISTRATION DETAILS:	
Company Registration/License No:	
Business License No./ Date of Issue	
License Issuing Authority	
Legal form of the Company (Proprietorship/ Private/Partnership/Public)	
OTHER DETAILS:	
Number of Agents/Subagents	LOCAL:_____ FOREIGN: _____
Name of External Auditors	

(please check yes/no)

	PART 2 -GENERAL AML POLICIES, PRACTICES AND PROCEDURES	**YES**	**NO**
1.	Has your institution developed written policies on Anti Money Laundering, Know Your Customer and Anti-Terrorist Financing?	☐	☐
2.	Has your institution been subject to any investigation, indictment, conviction or civil enforcement action related to money laundering and terrorism financing in the past five years by any authority?	☐	☐
3.	In addition to inspections by the government supervisors/regulators, does your institution have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?	☐	☐
4.	Does your institution have a policy prohibiting accounts/relationships with shell firms/agents? (Shell firm/agents are those which don't have physical existence)	☐	☐
5.	Does your institution have record retention practice procedures that comply with applicable law and AML Policy of Himalayan Bank Ltd.?	☐	☐
6.	Does your institution apply AML policies and practices to all agents/sub-agents and subsidiaries of your institution both in the home country and in locations outside of that jurisdiction?	☐	☐
	PART 3 -KNOW YOUR CUSTOMER, DUE DILIGENCE AND ENHANCED DUE DILIGENCE		
1.	Has your institution implemented systems for identification of clients?	☐	☐
2.	Does your institution have procedures to establish a record for each client noting their respective identification documents and know your customer information?	☐	☐
3.	Does your institution take steps to understand the normal and expected transactions of your customers based on its risk assessment?	☐	☐
	PART 4 -REPORTABLE TRANSACTIONS AND PREVENTION AND DETECTION OF TRANSACTIONS WITH ILLEGALLY OBTAINED FUNDS.		
1.	Does your institution have policies for the identification and reporting of transactions that are required to be reported to the authorities?	☐	☐
2.	Does your institution screen transactions of customers that deem to be significantly high risk?	☐	☐
3.	Does your institution have procedures to identify transaction structured to avoid large cash reporting requirements?	☐	☐
	PART 5 -TRANSACTION MONITORING/RECORD RETENTION		
1.	Does your institution have a monitoring program for suspicious or unusual activity of the customers?	☐	☐
2.	Does your institution and other sub agents keep record of KYC/ID documents of customers? If	☐	☐

	yes for how many years such records are retained? No of Years……..		
PART 6 -AML TRAINING			
1.	Does your institution provide AML training to relevant employees/Sub agents?	☐	☐
2.	Does your institution communicate new AML related laws or changes to existing AML related policies or practices to relevant employees/Sub agents?	☐	☐
3.	Please indicate the date of Last training conducted		
4.	Does your institution have an established audit and compliance review function to test the adequacy of AML and Terrorist Financing procedures?	☐	☐
5.	Does your institution employ agents to carry out some of the functions of your institution and if so does your institution provide AML training to relevant agents?	☐	☐

PART 8- COPY OF DOCUMENTS TO BE ENCLOSED IN SUPPORT			
1.	Financial Institution's License	☐	☐
2.	Article of Association	☐	☐
3.	Memorandum of Association	☐	☐
4.	AML/Compliance Policy	☐	☐
5.	Copy of compliance officer Designation (i.e. Minute, appointment letter etc.)	☐	☐
6	Organizational Chart with Names	☐	☐
7	Share holding pattern	☐	☐
8	List of Board of Directors and Senior management	☐	☐
9	Most recent Audit Report	☐	☐
10	List of Sub agents with updated address information	☐	☐
11	List of top ten Payout Agents with address	☐	☐
12	Training materials and attendance sheet of training programs conducted during last FY.	☐	☐

DECLARATION:

TO THE BEST OF MY KNOWLEDGE, THE ABOVE INFORMATION IS CORRECT, ACCURATE AND REFLECTIVE OF MY COMPANY'S ANTI MONEY LAUNDERING, COMBATING TERRORISM FINANCING AND SANCTIONS COMPLIANCE POLICIES, PROCEDURES AND PROGRAMS. ON REQUEST OF HIMALAYAN BANK LIMITED, WE WILL FURNISH THE DETAILS AND PARTICULARS OF ENHANCED DUE DILIGENCE PERFORMED ON THE TRANSACTION ROUTED THROUGH HIMALAYAN BANK LIMITED.

……

Authorised Signature (company Seal)

Name: _____

DESIGNATION: _____

TEL NO. : _____ FAX NO: _____

E-MAIL: _____ DATE: _____

ANNEXURE 6: AML/CDD REVIEW QUESTIONNAIRE FOR HIMAL REMIT SUB AGENTS

Himalayan Bank Limited

CDD/KYC Review of Himal Remit Sub-Agents

हिमाल रेमिट एजेन्टहरुको ग्राहक–पहिचान

एजेन्टको नाम :

एजेन्टको ठेगाना :

हिमाल रेमिटको एजेन्ट भएको मिति :

सम्बन्धित प्रिन्सिपल एजेन्ट :

व्यवसायको प्रकार : प्रोप्राइटर सिप/साझेदरी /अन्य.....

व्यवसाय दर्ता भएको निकाय :

व्यवसायको दर्ता नम्बर : प्यान नम्बर

दर्ताको म्याद सकिने मिति :

प्रोप्राइटर/साझेदार/संचालकहरुको नाम :

१.
२.
३.
४.
५.

संलग्न गर्नु पर्ने कागजातहरु

- दर्ता प्रमाण पत्रको प्रतिलिपि
- प्रोप्राइटर/संचालकहरुको नाम (लेटर प्याडमा)
- प्रोप्राइटर/संचालकहरुको नागरिकताको प्रतिलिपि
- मुख्य एजेन्ट संगको सम्झौताको प्रतिलिपि

हिमाल रेमिट बाहेक हाल प्रदान गरिरहेको अन्य सेवाको विवरण :

ग्राहकलाई नगद भुक्तानी तथा उनीहरुबाट नगद प्राप्त गर्दा के कस्तो परिचय पत्र लिने गरेको छ? यस्तो परिचय पत्र कति भन्दा माथिको नगद रकम प्राप्त गर्दा वा भुक्तानी गर्दा लिने गरेको छ?

परिचय–पत्रको प्रकार : न्यूनतम रकम :

ग्राहकलाई नगद भुक्तानी तथा उनीहरुबाट नगद प्राप्त गर्दा यदि कुनै ग्राहक शंकास्पद लागेमा सो को विवरण प्रिन्सिपल एजेन्टलाई दिने गरेको छ कि छैन?

छ छैन

यो विवरण भर्ने को नाम थर :

व्यवसाय संगको सम्बन्ध :

मिति : हस्ताक्षर :

(छाप)

For Bank's Use Only

Name(s) and Signature of Bank's Officials visiting Agents

Date:

Signature:

Name:

ANNEXURE 7: ALPA PROVISION ON TERRORIST, TERRORIST GROUP OR TERRORIST ORGANIZATION

***29E: Information of Terrorist, Terrorist Group or Terrorist Organization**:*

(1) The Ministry of Foreign Affairs shall decide to freeze the property of funds of person, group or organization designated under the provisions of the resolutions of United Nations Security Council dealing with terrorist financing or proliferation of weapons of mass destruction without delay. It shall also publish the updated list of such designated person, group or organization and send it to the Ministry of Finance by electronic means.

(2) The Ministry of Home Affairs shall, without delay, publish the updated list pursuant to section 29F. in its website.

(3) Natural Person, Ministry of Finance, Regulator, concerned agency, reporting entity or any other legal person or legal arrangement shall ensure that they are aware of the updated lists of person, group or organization referred to in subsection (1) by regularly consulting the lists referred to subsections (1) and (2) and perform necessary actions as per this Act.

(4) After getting the list or information of the listed person, group or organization in accordance with subsection (2) and (3), the Ministry of Finance, concerned Regulator shall inform agencies under it or regulated by it about such person, group or organization immediately and shall regularly upload or disseminate such list their respective websites.

***9F: Listing as a Terrorist, Terrorist Group or Terrorist Organization**:*

(1) The Ministry of Foreign Affairs, if it receives a request from a foreign country in order to freeze the property or fund of a person, group or organization suspected of being a terrorist or terrorist group or Organization, shall send such request to the Ministry of Home Affairs without delay.

(2) The Ministry of Home Affairs shall make necessary inquiry against a person, group or organization involved or suspected of involving in terrorist act either upon the receipt of request pursuant to subsection (1) or of Nepali or foreign citizen, group or organization involved in or having reasonable grounds of suspicion of being involved in terrorist act inside or outside of Nepal, in its own initiative.

(3) The Government of Nepal may designate a person, group or organization as a terrorist, terrorist group or organization, if it finds or has reasonable grounds to believe that such person, group or organization is involved or going to be involved in the activities stipulated in subsection (2) or of section 4 or in any terrorist act pursuant to prevailing laws under prevailing laws, upon the inquiry made pursuant to subsection (2).

(4) The Government of Nepal may delist a person, group or organization listed pursuant to subsection (3) if it does not find grounds for keeping such person, group or organization into such list.

(5) The Ministry of Home Affairs shall, if any person, group or entity is delisted by the Government of Nepal pursuant to subsection (4), immediately publish its notice in its website.

***9G. Freezing of Fund or Property**:*

(1) Natural Person, concerned agency, Bank shall immediately and without delay, freeze the property or funds of a person, group or organization listed pursuant to section 29E., 29F. and of person, group or organization engaged or financing in the proliferation of weapons of mass destruction.

(2) While freezing the property or funds in accordance with subsection (1), all the following property of fund shall be frozen: -

(a) All property or funds belonging to or wholly or jointly, directly or indirectly, owned or possessed or held or controlled by such person, group or organization,

(b) All property or funds derived or generated from the property or funds pursuant clause (a), 28 (c) All property or funds of a person, group and organization acting on behalf of, or at the direction of such person, group or organization.

(3) Natural or legal person, legal arrangement, concerned agency or reporting entity shall make necessary management that the property or funds frozen pursuant to subsection (1) and (2) shall not be, directly or indirectly, available or in use of or be beneficial to the terrorist, terrorist group or terrorist organization and also to the person, group or organization related with the proliferation of weapons of mass destruction or of its financing and that shall be frozen in such a way that such property or instrumentality could not be transferred, mortgaged or sold or distributed or transacted by anyone, except in the execution of the provision of this Act and rules there under.

(4) Natural or legal person, legal arrangement, concerned agency shall send the report of such freezing pursuant to subsection (1) and (2) to the Ministry of Finance and reporting entity to the Regulator within three days of freezing.

(5) Regulator shall submit the detail of the freezing of the property or funds received pursuant to subsection (3) to Ministry of Finance within three days.

(6) Other additional provisions regarding freezing of property or funds shall be as prescribed.

***29H. De-freezing of Property and Funds**:*

(1) Any person affected by freezing made pursuant to section 29G. may submit application to the authority deciding on such freezing.

(3) Other provisions regarding the effective implementation of United Nations Security Council Resolutions including listing or delisting of terrorist, terrorist group, terrorist organization Pursuant to section 29G, or de-freezing of property or funds frozen pursuant to section 29G, appealing against the listing and freezing, proper protection of bona-fide third party, providing minimum property or funds for the subsistence of person whose property or funds is frozen and to give effect to other necessary measures to effectively implement the such UNSCRs shall be as prescribed.

***29I. Request to Another Country**:*

g. The Ministry of Home Affairs shall immediately send the list of person, group or organization listed pursuant to section 29F. through the Ministry of Foreign Affairs with a request to freeze such fund or property if it finds that property or funds of such person, group or organization may be located in another country.

(2) The Ministry of Home Affairs shall send the name of person, group or organization if it is delisted through the Ministry of Foreign Affairs in order to defreeze property or funds frozen pursuant to subsection (1).

***29J. Monitoring**:*

1. The National Coordination Committee shall make overall monitoring and evaluation about the effective compliance of this chapter.

(2) Concerned Ministry shall regularly monitor whether the concerned agencies have effectively implemented the provisions of this chapter.

(3) Regulator shall regularly monitor whether the reporting entities have effectively implemented the provisions of this chapter.

(4) Other provisions for the monitoring under this section shall be as prescribed.

***29K. Sanctions**:*

(1) Regulator may impose sanction pursuant to section 7T if it finds any reporting entity is not freezing the property or funds pursuant to section 29H.

(2) Departmental action shall be taken to the officials of the concerned agency not freezing the property or funds pursuant to section 29G.

(3) The Ministry of Home Affairs may fine up to one million rupees to a natural or legal person violating the section 29H.

29 (4) Notwithstanding whatever written in the subsection (1), (2) or (3), case of ML or TF may be filed against a natural person, legal person or responsible official of concerned agency or reporting entity who does not freeze the property or funds with an intention to support the commission of offence of ML or TF.

(4) The provisions, under this Act, for tracing property and instrumentality, freezing, seizing, investigation and confiscation of the property or funds of terrorist, terrorist group or organization and other shall be applicable to offenses under this chapter if so required.

***30.Punishment in the offense of Money laundering or Terrorist Financing**:*

(1) Any person who has committed the offense of money laundering pursuant to subsection (1) of section 3 shall be fined two times of the proceeds and imprisoned from two years to ten years.

(2) Any person who has committed any offense of conspiracy to commit the money laundering pursuant to subsection (2) of section 3 shall be punished pursuant to subsection (1) and person committing other offenses under the subsection (2) of section 3 shall be punished half of the subsection (1).

(3) Any person who has committed any offense of terrorist financing pursuant to subsection (1) of section 4 shall be imprisoned from three years to twenty years and fined five times of the Proceeds if it is apparent or fined up to ten million NRs if such proceeds is not apparent.

(4) Any person who has committed the offense pursuant to subsection (2), (3) or (4) of section 4 shall be half of the subsection (3).

(5) If a person commits the offense of ML/TF through or by the use of a legal person, such person, official or staff shall be punished pursuant to subsection (1), (2), (3) or (4).

(6) The chief of legal person working during the period of commission of the offense shall be punished pursuant to prevailing laws if the particular person committing such offense is not traced out.

(7) Punishment to a public servant or chief or staff of a reporting entity shall be punished ten percent more of the punishment stipulated in subsections (1), (2), (3) or (4) if he is found to have committed the offense of ML/TF.

(8) If any legal person or arrangement commits any offense of money laundering or terrorist financing, one or all following punishment shall be awarded on the basis of the gravity of offense: -

- *(a) Fine up to five times of the fine stipulated in subsection (1), (2), (3) or (4), and/or*
- *(b) Prohibiting in public procurement by prescribing time limit*
- *(c) Prohibiting in subscribing goods and services by prescribing time limit*
- *(d) Recovering losses and damages*
- *(e) Cancel or evoke license or permission,*
- *(f) Liquidating legal person.*

(9) If any anyone, who violates any provision of this Act and rules issued there under beyond subsection (1) to (7), shall be punished with the confiscation of property and fine equal to that, and if the property is not apparent or fine up to one million NRs.

***31.Punishment to the Discloser of confidentiality**:*

Anyone who violates the confidentiality pursuant to subsection (2) of section 10B. or section 26 shall be punished with imprisonment from one month to three months or fine up to one hundred thousand or both.