एभरेष्ट बैंक
EBL EVEREST BANK
Consistent · Strong · Dependable

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

KYC/AML/CFT POLICY - 2026

Know Your Customer / Anti Money Laundering / Combating Financing of Terrorism Policy

May 2026

Everest Bank Limited
Compliance Department
4th Floor, Baneshwor Building
New Baneshwor, Kathmandu
Bagmati, Nepal

KYC/AML/CFT Policy - 2026

EVEREST BANK LIMITED

May 2026

Owner : Compliance Department
Version : 11.0

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

Total Number of Pages : 33
(Including table of contents & covering pages)

PREAMBLE

Know Your Customer/Anti Money Laundering/ Combating Financing of Terrorism Policy (KYC/AML/CFT Policy), 2025

In terms of the provisions of Asset Laundering (Money Laundering) Prevention Act, 2064 (2008) and Asset Laundering (Money Laundering) Prevention Rules, 2081 (2024), as amended from time to time by the Government of Nepal and Nepal Rastra Bank Unified Directives/Circulars and amendments thereof issued from time to time, the Bank is required to follow certain customer identification procedure while undertaking a transaction either by establishing an account based relationship or otherwise and monitor their transactions.

In exercise of the power conferred by Section 22 (3) of Bank and Financial Institution Act 2073 and the Articles of Association of Everest Bank Limited, the Board of Directors (BOD) of Everest Bank Limited has approved this "Know Your Customer/Anti Money Laundering/ Combating Financing of Terrorism Policy (KYC/AML/CFT Policy – 2026)" vide its 398th Board Meeting dated 22th May 2026 for implementation after review and recommendation of 4th Asset Laundering Prevention Committee (ALPC) meeting for FY 2082/2083 held on 22nd February 2026.

The core purpose of this policy document is to lay down a framework for Know Your Customer, Anti Money Laundering and Combating Financing of Terrorism, and provide guidelines on KYC/AML/CFT compliance across all the functions of the Bank to mitigate the compliance and subsequent operational risk.

All offices of the Bank shall take all necessary steps to implement this KYC policy and provisions of Asset Laundering (Money Laundering) Prevention Act, 2064 (2008) and Asset Laundering (Money Laundering) Prevention Rules, 2073 (2016), as amended from time to time and Nepal Rastra Bank Unified Directives/Circulars and amendments thereof issued from time to time, including internal operational guidelines/instructions issued in pursuance of such amendment(s).

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

POLICY CUSTODIAN

Department	**Compliance Department**
Officer In-Charge	**Compliance Officer**
Policy Contact	**complianceofficer@ebl.com.np**

VERSION CONTROL

S.N.	Version Control No.	Date of Approval	Approving Authority	Remarks
1	Version 1	June 15, 2015	257thBoard	Revised
2	Version 2	April 07, 2017	278th Board	Revised
3	Version 3	November 01, 2018	298th Board	Revised
4	Version 4	October 13, 2019	310th Board	Revised
5	Version 5	October 9, 2020	321st Board	Revised
6	Version 6	January 07, 2022	336th Board	Revised
7	Version 7	February 10, 2023	348th Board	Revised
8	Version 8	February 12, 2024	363rd Board	Revised
9	Version 9	February 26, 2024	364th Board	Revised
10	Version 10	March 06, 2025	380th Board	Revised
11	Version 11	May 22,2026	398th Board	Revised

POLICY GOVERNANCE

Frequency of Review	Annually
Approving Authority	The Board
Date of Approval	22nd May 2026
Last Reviewed on	06th March 2025
Approval Path	CO-CH-DGM-CEO-ALPC-BOARD
Supersedes	KYC-AML-CFT Policy 2025 dated 06.03.2025

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

INDEX

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

KYC/AML/CFT POLICY- 2026

1. INTRODUCTION

1.1 It is extremely important to ensure that funds generated through illegal and criminal activities are not channeled within the financial system of a country irrespective of its origin. The Financial Action Task Force (FATF) established by G7 group of countries has come up with strong recommendations (40 recommendations) against illegal and 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 and an associate member of FATF), it is the duty of Nepalese bank to check and control money laundering related activities.

1.2 The "Asset Laundering (Money Laundering) Prevention Act, 2064 B.S. (2008)" prohibits financial Institutions to collect deposit (fund) from customers that have been generated from illegal and criminal source. Furthermore, the institutions should not be involved even in helping customers to conceal, transform, transfer, hide its source or misrepresent about it and immediately inform details of such fund/transaction to the "Financial Intelligence Unit (FIU)".

1.3 Everest Bank Limited ("the Bank") has in placed Board approved KYC/AML/CFT Policy. The policy has been reviewed/updated taking into cognizance of Assets Laundering (Money Laundering) Prevention Act (ALPA) 2064 B.S. (2008), Assets Laundering (Money Laundering) Prevention Rules (ALPR) 2081 B.S. (2024), Unified Directives/Circulars on AML/CFT issued by Nepal Rastra Bank (NRB) and Financial Intelligence Unit (FIU) TTR and STR Guidelines.

2. OBJECTIVES OF THE POLICY

2.1. To lay down policy framework for abiding by the Know Your Customer Norms, AML and CFT Measure as set out by NRB, based on the provisions under ALPA and ALPR.

2.2. To prevent the Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or financing terrorist activities to protect the bank's reputation.

2.3. To enable the Bank to know/understand its customers and their financial dealings better by conducting Due Diligence so as to manage its risks prudently.

2.4. To have adequate controls and systems in place to mitigate the risk of being used for money laundering or financing terrorist activities.

2.5. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures and regulatory guidelines.

2.6. To take necessary steps to make the dealing staffs adequately trained in KYC/AML procedures and protect them from unforeseen risks from money laundering activities.

2.7. To provide a broad framework for formulation and implementation of procedural guidelines required for effective KYC/AML/CFT compliance.

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

3. SCOPE OF THE POLICY

3.1. This policy is applicable to all branches, offices, representatives posted at abroad and Representative Office, New Delhi, India (Rep. Office, New Delhi) of the Bank and is to be read in conjunction with related procedural guidelines issued by the management from time to time for implementation of this policy. In case of Representatives posted at abroad and Rep. Office, New Delhi, if there is a variance in KYC/AML standards prescribed by the Nepal Rastra Bank and the host country regulators, the more stringent regulation of the two shall be adopted.

3.2. The contents of the policy shall always be read in tandem/auto-corrected with the changes/modifications which may be advised by NRB, FIU-Nepal (NRB) and / or by ALPA/ALPR (and its amendments)/ or by the Bank through internal operational guidelines/instructions/circulars from time to time.

4. DEFINITIONS AND EXPLANATIONS OF VARIOUS TERMS

Unless otherwise specifically indicated, the following terms used in Policy shall have the following meaning(s):

4.1 Customer

For the purpose of Policy, a 'Customer' is defined as a person or entity that maintains or tries to maintain an account and/or has a business relationship with the bank. A Beneficial Owner and/or Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

4.2 Know Your Customer (KYC)

KYC is the process of a business verifying the identity of its customers. It is to safeguard the bank's interest from the hands of fraudsters and to understand their customers and their financial needs cautiously and also to eliminate money laundering or money reaching the hands of terrorists.

4.3 Beneficial Owner (BO)

A Beneficial Owner (BO) is a natural person who directly or indirectly owns or controls or directs or influences customers, transactions, assets, legal person or legal arrangement or remains as an ultimate beneficiary or owner. It is a human being and distinct from a legal person, e.g. an entity. The BO are the individuals who

i. ultimately own or hold (either directly or indirectly through one or more shareholdings) 15 percent or more of the issued capital or its voting rights, or
ii. exercise ultimate control over the management of the entity, or
iii. exercise significant influence (directly or indirectly) in the entity, customer or their assets, or on whose behalf a transaction is being conducted

4.4 High Level Person (Politically Exposed Persons i.e. PEPs)

High Level Person (PEPs) means domestic high-level officials or persons, foreign high-level officials or persons or high-level officials of international organizations. It shall also include other group of persons as designated by the Government of Nepal by publishing notice in Nepal Gazette at the recommendation of National Coordination Committee.

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

The PEPs shall be classified into the following categories:

a. Current Domestic PEPs
b. Former Domestic PEPs
c. Neighboring (China) & SAARC Countries PEPs
d. Other Country PEPs (Other than China and SAARC Countries)
e. PEPs of International Organization

4.5 Current Domestic Politically Exposed Person (CD-PEPs)

A current domestic Politically Exposed Person (CD-PEPs) is an individual who currently holds a prominent public position or has been entrusted with prominent public functions within the country. It can include heads of Central, Province or Local judicial officials, senior politicians, senior government officials, military officials, senior executives of state-owned corporations, and important political party officials.

The current domestic PEPs are considered high-risk clients in financial transactions due to their potential involvement in corruption, money laundering and other financial crimes. The Branches are required to apply enhanced due diligence measures when dealing with CD-PEPs to mitigate these risks.

4.6 Former Domestic Politically Exposed Person (FD-PEP)

A Former Domestic Politically Exposed Person (FD-PEP) is an individual who previously held a prominent public position or entrusted with prominent public functions within the country but now no longer holds that position or function. The definition typically includes former heads of state, former senior politicians, former heads of state-owned companies, former senior military officials, former senior government officials, former important political party officials.

The status of a former domestic PEP usually lasts for 10 years after they leave their office or retire from their position or function. During this period, they are still considered high-risk clients in financial transactions due to their potential involvement or influencing position in corruption, money laundering, and other financial crimes. The Branches are required to apply enhanced due diligence measures when dealing with FD-PEPs to mitigate these risks.

4.7 Neighboring (China) & SAARC Countries PEPs

Politically Exposed Persons (PEPs) from neighboring countries like China and SAARC countries (Afghanistan, Bangladesh, Bhutan, India, Maldives, Pakistan, and Sri Lanka) include individuals who hold or have held prominent public positions. These positions can make them vulnerable to corruption and other financial crimes. The Branches are required to apply enhanced due diligence measures when dealing with Neighboring (China) & SAARC Countries PEPs to mitigate these risks.

4.8 Other Country PEPs (Other than China and SAARC Countries)

Politically Exposed Persons (PEPs) other than from China and SAARC countries (Afghanistan, Bangladesh, Bhutan, India, Maldives, Pakistan, and Sri Lanka) who hold or have held prominent public positions are Other Country PEPs (Other than China and SAARC Countries). These positions can make them vulnerable to corruption and other financial crimes. The Branches are required to apply enhanced due diligence measures when dealing with Other Country PEPs (Other than China and SAARC Countries) to mitigate these risks.

4.9 PEPs of International Organization

Politically Exposed Persons (PEPs) of International Organizations are individuals who hold or have held prominent positions within these organizations. These positions can make them vulnerable to corruption and other financial crimes.

International Organizations include organizations with universal membership of sovereign states, established by treaties that provide them with legal status. Examples include the United Nations (UN) and its specialized agencies like Food and Agriculture Organization (FAO), International Civil Aviation Organization (ICAO), International Fund for Agricultural Development (IFAD), International Labor Organization (ILO), International Monetary Fund (IMF), United Nations Educational, Scientific and Cultural Organization (UNESCO), World Health Organization (WHO), World Bank Group, World Meteorological Organization (WMO) and World Trade Organization (WTO). It should also include regional organization like NATO, the European Union, African Union, Organization for Security and Co-operation in Europe (OSCE) and the Commonwealth of Nations.

The Branches are required to apply enhanced due diligence measures when dealing with PEPs of International Organization.

4.10 Relatives and Close Associates (RCAs)

Relatives i.e. Family members of PEPs are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership. Close associates are individuals who are closely connected to PEPs, either socially or professionally.

4.11 Walk in Customers

Walk-in Customer means a person who does not have an account-based relationship with the Bank but undertakes transactions with the Bank.

4.12 Non-Face to Face Customers

Non-face-to-face customers means customer who do business relationships without visiting the branch / offices of the Bank or meeting the officials of the Bank.

4.13 Non-Resident Customers

Non-resident customers mean customers primarily resident in a different jurisdiction to the location where bank services are provided.

4.14 Money Laundering

Money laundering is the process by which the person attempts to hide and disguise the true origin and ownership of the proceeds of their unlawful activities. The term" Money Laundering" is also used in relation to the financing of terrorist activity (where the funds may, or may not, originate from crime). There are three stages of Money Laundering namely Placement, Layering and Integration.

4.15 Financing of Terrorism

Financing of Terrorism means providing financial support to any form of terrorism or to those who encourage terrorism. Funds may stem from legal and illegal sources. According to the International Convention for the Suppression of the Financing of Terrorism, a person commits the crime of financing of terrorism "if the person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the

CONFIDENTIAL FOR INTERNAL CIRC

knowledge that they are to be used, in full or in part, in order to carry out" an offense within the scope of the Convention.

4.16 Proliferation Financing (PF)

Proliferation Financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials that would contribute to the Weapons of Mass destruction (WMD) proliferation (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. Bank shall work towards raising awareness and be watchful to providing funds or financial services which are not intended towards proliferation and proliferation financing of WMD.

4.17 Targeted Financial Sanctions (TFS)

TFS means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities. The United Nations Security Council (UNSC) imposes TFS against specific individuals and entities identified by the UN Security Council Resolutions (UNSCRs) 1267 and its subsequent resolutions, 1373 and its subsequent resolutions or relevant UN Committees as contributing to a particular threat to, or breach of, international peace and security.

4.18 Shell Entity

Shell Entity is a company that is incorporated but has no assets or operations. A Shell Entity serves as a vehicle for business transactions without having any significant assets or operations of their 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.

4.19 Offshore Bank

Offshore Bank is a bank located outside the country of residence of the depositor, typically in a low tax jurisdiction or tax haven that provides financial and legal advantages. It is having a banking transaction in a location outside the country one is residing in.

4.20 Correspondent Banking

Correspondent banking is an agreement between two banks whereby one bank (correspondent bank) carries on representative services for another bank (respondent bank). It refers to a financial institution that provides services to another one - usually in another country. It acts as an intermediary or agent, facilitating wire transfers, conducting business transactions, accepting deposits, and gathering documents on behalf of another bank. Correspondent banks are most likely to be used by domestic banks to service transactions that either originate or are completed in foreign countries. Domestic banks generally use correspondent banks to gain access to foreign financial markets to serve international clients without having to open branches abroad.

4.21 Downstream Correspondent Banking (Nested accounts)

Nested Accounts occur when a financial institution accesses the financial system in another country (in effect anonymously) by operating through a correspondent banking account belonging to another financial institution.

FINAL FOR INTERNAL CIRCULATION ONLY

4.22 Payable-through Accounts (“Pass-through” or “Pass-by” accounts)

Payable-through accounts are demand deposit accounts maintained at financial institutions by foreign banks or corporations. The foreign bank funnels the deposits and cheques of its customers (usually individuals or businesses located outside the country) into a single account that the foreign bank holds at the local bank. The foreign customers have signing authority over the account as sub-account holders and can thereby conduct normal international banking activities.

4.23 Risk Based Approach

A risk-based approach means banks identify, assess, and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk taking into account national risk assessments and legal and regulatory framework.

This flexibility allows for a more efficient use of resources, as banks can decide on the most effective way to mitigate the money laundering / terrorist financing risks they have identified. It enables them to focus on their resources and take enhanced measures in situations where the risks are higher, apply simplified measures where the risks are lower and exempt low risk activities.

4.24 Periodic Review

Periodic Review means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed in this Policy.

4.25 Simplified Customer Due Diligence (SCDD)

Simplified Customer Due Diligence is the process of identifying and evaluating the low risk graded customer having annual transactions of rupees one lac and below or as defined by the regulator.

4.26 Customer Due Diligence (CDD)

Customer Due Diligence is identifying and verifying the customer and the beneficial owner. It is the process of identifying and evaluating the customer and reassessment of customer risk as part of Know Your Customer (KYC) process, allowing banks to better identify, manage and mitigate the AML related risks. This is conducted for Low risk and Medium risk customers.

4.27 Enhanced Customer Due Diligence (ECDD)

Enhanced Customer Due Diligence refers to additional due diligence pertaining to the customer when a risk-based approach to CDD will identify situations in which there is a higher risk of ML/TF. This is conducted for high-risk customers.

It shall include the following:

a. Obtaining additional information such as additional identifying information, residential proof etc. on the customer and its ultimate BOs;
b. Obtaining additional information on the intended nature of the business relationship;
c. Obtaining information on the source of wealth and source of funds of the customer and the customer’s BO;
d. Where there is a deviated profile, obtaining information on the reasons for the transaction;

CONFIDENTIAL - FOR INTERNAL CIRC

e. Obtaining the approval of senior management for establishing or continuing the business relationship.

4.28 Senior Management

For the purposes of KYC/AML/CFT Compliance, Senior Management refers to officials at the level of Assistant General Manager (AGM) and above. This designation also includes Province Managers and any other authority duly approved by the CEO.

4.29 Trigger Event

A trigger event is some new event or piece of information that alters the information in the CDD record and would cause it to be reviewed e.g. significant adverse/negative media news, or disclosure of a regulatory order.

4.30 Financial Action Task Force (FATF)

The FATF was established in 1989 by the G-7 countries to combat ML/TF. It is an inter-governmental body which sets international standards to combat money laundering and terrorist financing, which are binding and applicable to all its members jurisdictions, regional organizations and observers. The FATF Plenary, the decision-making body, meets three times a year around February, June and October and identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in two FATF public documents that is "High Risk Jurisdiction - Call for Action" and "Other Monitored Jurisdictions/Jurisdictions under Increased Monitoring".

4.31 Asia/Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organization founded in 1997 in Bangkok, Thailand consisting of 41 members and a number of APG observers. Some of the key international organizations who participate with and support the efforts of the APG in the region include the Financial Action Task Force, International Monetary Fund, World Bank, OECD, United Nations Office on Drugs and Crime (UNODC), Asian Development Bank (ADB) and the Egmont Group of Financial Intelligence Units.

APG members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the 40 recommendations of the Financial Action Task Force (FATF). Nepal became a member of APG in June 2002.

4.32 High Risk Jurisdiction - Call for Action (FATF Blacklist)

High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and in the most serious cases, countries are called upon to apply countermeasures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country. This list is often externally referred to as the "blacklist".

4.33 Other Monitored Jurisdictions/Jurisdictions under Increased Monitoring (FATF Grey List)

Jurisdictions under increased monitoring are actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

proliferation financing. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the 'grey list'. The FATF does not call for the application of enhanced due diligence to be applied to these jurisdictions but encourages its members to take into account the provided information in their risk analysis.

4.34 Financial Intelligence Unit (FIU)

In order to work against the money laundering and terrorist financing activities Financial Intelligence Unit (FIU) was established on April 21, 2008 pursuant to section 9 of the Assets (Money) Laundering Prevention Act, 2008 within Nepal Rastra Bank (the Central bank) as an independent unit. It is Nepal's financial intelligence unit. It is a central, national agency responsible for receiving, processing, analyzing and disseminating financial information and intelligence on suspected money laundering and terrorist financing activities.

4.35 Predicate Offences

Predicate offences are the crimes underlying ML/TF activities. The various types of predicate offences shall be as mentioned in the annexure of the Asset Laundering (Money Laundering) Prevention Act, 2064 (2008).

4.36 Wolfsberg Group Correspondent Banking Due Diligence Questionnaire (CBDDQ)

Wolfsberg Group is a non-governmental organization founded in AD 2000 at the Chateau, Wolfsberg in northeastern Switzerland. It is an association of 13 large global banks which aims to develop frameworks and guidance for the management of financial crime risk particularly with respect to Know Your Customer (KYC), Anti-money laundering (AML), and Counter Terrorist Financing (CTF) policies. The Wolfsberg Group has revised its previous Anti-Money Laundering Questionnaire for Correspondent Banks. The new Wolfsberg Correspondent Banking Due Diligence Questionnaire (CBDDQ) has been comprehensively updated, refined and restructured to cover all main aspects required to conduct effective correspondent banking due diligence.

4.37 US Patriot Act Certification

USA PATRIOT Act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." Pursuant to the USA Patriot Act and the final rules issued by the U.S. Department of Treasury, a U.S. bank (a "Covered Financial Institution") is required to obtain a Certification from any "Foreign Bank" that maintains a correspondent account with it.

4.38 FATCA

FATCA" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions (FFI) to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

5. POLICY FRAMEWORK, COMPLIANCE PROGRAM AND STANDARDS

The bank shall follow the international and domestic legal framework.

CONFIDENTIAL FOR INTERNAL CIRCULATION ONLY

INTERNATIONAL FRAMEWORK

a. **FATF:** The FATF assesses countries against a set of recommendations (the 40 Recommendations) that represent best practices for AML/CFT systems. The Financial Action Task Force (FATF) 40 recommendations issued on 2012 and regularly updated since (Last updated in November 2023) has set minimum standards for action for countries to implement according to their particular circumstances and the applicable domestic legal frameworks pertaining to AML/CFT. The FATF Recommendations cover all the, measures that national systems should have in place within their criminal justice and regulatory systems: the preventive measures to be taken by financial institutions and certain other businesses and professions: and international co-operation.

b. **APG:** The Asia Pacific Group (APG) deals with Anti Money Laundering and Combating the Financing of Terrorism and is a FATF Style Regional Body (FSRB). FSRB's perform a similar function as the FATF on a regional basis. Nepal is a member of the APG and is subject to the assessment of its AML/CFT framework by the APG.

The recommendations of FATF, APG and other functional bodies like IMF and World Bank shall be taken care of by the Bank as applicable.

DOMESTIC LEGAL FRAMEWORK

The applicable domestic legal frameworks pertaining to AML/CFT are as follows:

a. Asset Laundering (Money Laundering) Prevention Act, 2064 (2008) (Including amendments)
b. Asset Laundering (Money Laundering) Prevention Rules, 2081 (2024)
c. Asset Laundering (Money Laundering) Prevention (Freezing of Properties and Funds of Designated Person, Group and Organization) Rules 2070 (2013)
d. Unified Directives No. 19 issued by Nepal Rastra Bank
e. Ministry of Home Affairs Targeted Sanction List of Designated Person, Group and Organization
f. FIU Threshold Transactions Reporting Guidelines to Banks & FIs.
g. FIU Suspicious Transactions Reporting and Suspicious Activity Reporting Guidelines to Banks & FIs.

COMPLIANCE PROGRAM AND STANDARDS

This policy sets out the minimum compliance program and standards which must be complied with and includes:

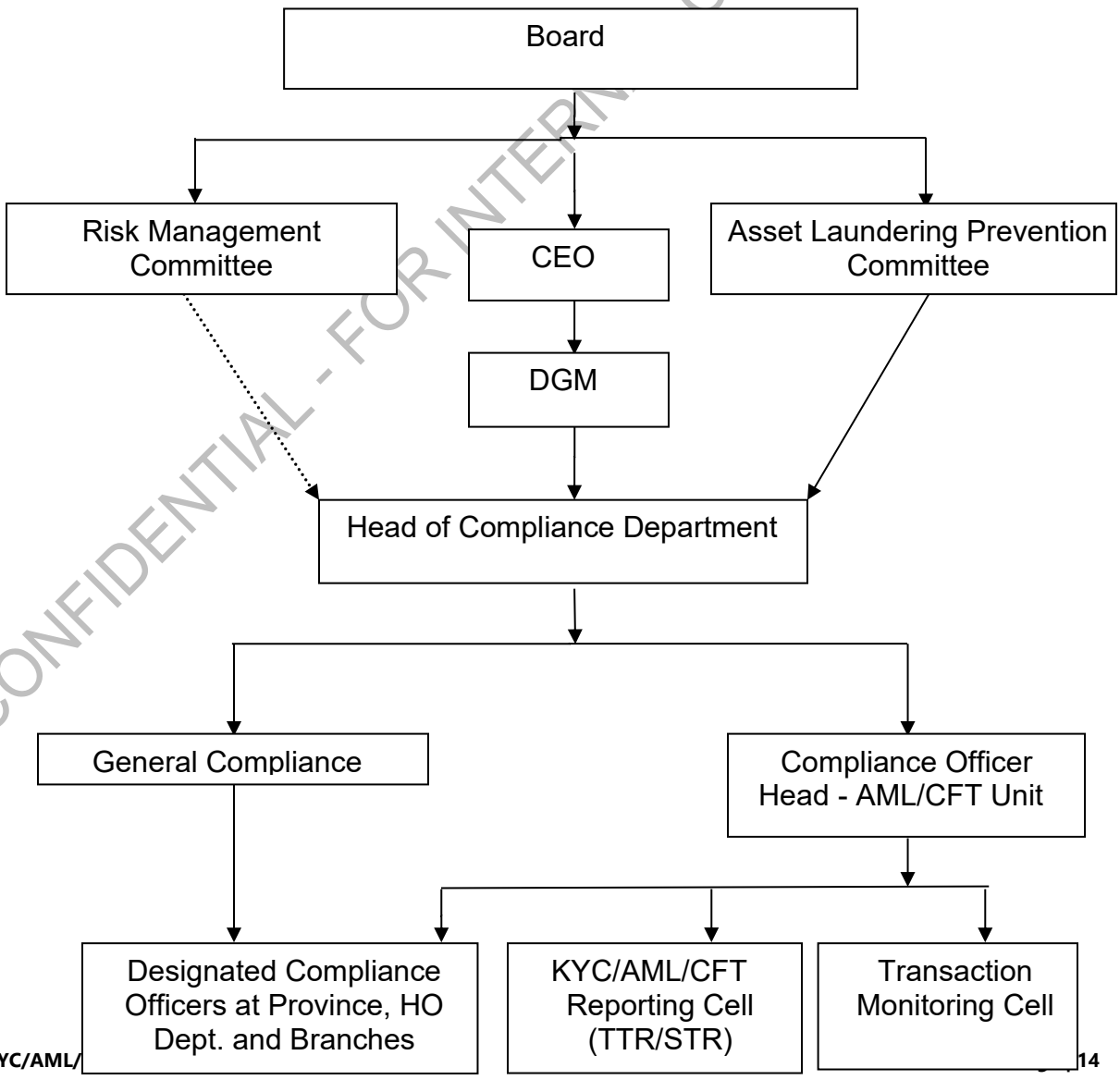
- The appointment of a Compliance Officer who has sufficient level of seniority, experience and independence.
- Formulation and periodic review of Policies and Procedures to combat ML/TF.
- Approval of KYC/AML/CFT/Sanctions Policy at least annually by the Board.
- Approval of KYC/AML/CFT/Sanctions Procedures by the CEO.
- Approval of Name Screening Process by the CEO.
- Establishing and maintaining a Risk Based Approach towards assessing and managing the money laundering and terrorist financing risks to the bank.
- Establishing system for Sanctions Screening, PEPs & RCAs Identification/Screening, Enforcement and Negative Media Screening of new and existing customers.
- Identification of Beneficial Ownership

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

- Establishing and maintaining risk-based customer due diligence (CDD), identification, verification and know your customer procedures, including application of enhanced due diligence (EDD) for those customers presenting higher risks, such as Politically Exposed Persons (PEPs).
- Establishing Transaction Monitoring System and maintaining risk based systems and procedures to monitor on-going customer transactions.
- Procedure for reporting Threshold Transactions Reports
- Procedure for reporting suspicious transactions/activity internally and to the FIU, NRB.
- The maintenance of appropriate records for the minimum prescribed periods.
- Training and awareness for all relevant employees.
- Independent Testing by the Internal Audit Department to ensure adequacy and effectiveness of KYC/AML/CFT/Sanctions Program and standards.
- Periodic Reporting to Management and Board on the status of KYC/AML/CFT/Sanctions Program and standards.
- Conduct the Institutional ML/TF Risk Assessment of the Bank annually and amend the KYC/AML/CFT Procedure accordingly to mitigate the ML/TF risk.

6. COMPLIANCE STRUCTURE

For effective management of Compliance Risk, the Bank has established a Compliance Structure as follows:



CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

7. ROLE AND RESPONSIBILITIES OF VARIOUS BODIES INVOLVED IN KYC, AML & CFT COMPLIANCE

7.1 BOARD OF DIRECTORS SHALL:

7.1.1. Encourage regulatory and internal compliance

7.1.2. Ensure an appropriate KYC, AML & CFT policy is in place in the bank to manage the ML and TF risk.

7.1.3. Approve KYC, AML & CFT policy recommended by the ALPC.

7.1.4. Approve Annual Program and Budget for KYC, AML & CFT recommended by the ALPC.

7.1.5. Review and Approve ML/TF risk assessment Report.

7.1.6. Determine the Bank's risk appetite on Customer Acceptance;

7.1.7. Be in active engagement with the senior management for establishing internal controls.

7.1.8. Ensure that senior management is taking necessary steps to identify, measure, monitor and mitigate the ML/TF risks including implementing strategies to mitigate those risks

7.1.9. Have oversight over the ML and TF risk through various reports placed by the various bodies involved in KYC, AML & CFT compliance.

7.2 ASSET LAUNDERING PREVENTION COMMITTEE SHALL

7.2.1 Placing the report to the Board after reviewing the bank's activities/performance conducted as per the terms of Assets Money Laundering Prevention Act 2064, Assets Money Laundering Rules 2081 and NRB, Unified Directives Chapter 19.

7.2.2 Framing requisite policy and implementing it after having discussion on the adequacy of placed and implemented policy, procedure and process as per the terms of Assets Money Laundering Prevention Act 2064, Assets Money Laundering Prevention Rules 2081, NRB Unified Directives Chapter 19 and Financial Action Task Force Recommendations.

7.2.3 Placing recommendation to the board for improving procedural arrangement and information technology placed and to be placed to identify and prevent assets laundering and financing on terrorist activity.

7.2.4 Analyzing customer identification process and forming Customer Acceptance Policy for effective implementation of identification of High-level individuals (PEPs), Beneficial Owner etc. as per risk classification.

7.2.5 Submitting quarterly report to the board on compliance and status of implementation of Assets Laundering Prevention Act, Rules, NRB directives and internal policy, guidelines.

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

7.2.6 Discussing and placing recommendations as per the requirement to the board on the following:

a. Report on AML/CFT risk management.

b. Updated status of customer identification, details on Customer Due Diligence (CDD), Details of PEPs and Enhanced Customer Due Diligence (ECDD) and steps to be taken for efficacy of the process using information technology in future.

c. Details of procedural arrangement required for improvement reviewing observation of internal audit, statutory audit and inspection report of Nepal Rastra Bank on assets laundering and terrorist financing.

7.2.7 Details on procedural arrangement required for mitigating risk of assets laundering and terrorist financing associated with online and offline transaction and transfer of money through launched new product and services, acquired IT system, E-banking/mobile banking, QR code, mobile wallet etc.

7.2.8 Placing recommendation for risk management to the board analyzing the national and international issues and incidences related with assets laundering and terrorist financing and its likelihood impact on the bank.

7.2.9 Managing Knowledge Transfer Training program for delivering suitable knowledge on AML/CFT to Compliance Officer, Shareholders holding 2% or more shares of the bank, board directors, senior executives and the staff members directly and regularly involving on AML/CFT.

7.2.10 Placing recommendation to the board on the adequacy of internal policy and guidelines reviewing internal policy and procedure placed on assets laundering and terrorist financing regularly.

7.2.11 Ensuring effective implementation of AML/CFT system, risk management, adequately monitored unnatural activities and submitting required report to the concern authority and making arrangement for discussing these topics on the board.

7.2.12 Discussing on report submitted to Financial Information Unit and other agency as instructed by NRB on assets laundering and terrorist financing whether such reports are submitted as per the requirement complying with the 44 Ka provision made by the Assets Money Laundering Prevention Act, 2064.

7.2.13 Getting the Annual Budget and Program approved from the Board for doing the AML/CFT activities on risk-based approach and required to develop the system to ensure the effective implementation of Board approved annual program and regularly monitor the same.

7.3 MANAGEMENT SHALL:

7.3.1 Oversee implementation and manage the ML & TF risk faced by the Bank.

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

7.3.2 Appoint and inform the name and details of the Compliance Officer as also any change thereof, as and when it takes place to FIU and Nepal Rastra Bank, Bank Supervision Department.

7.3.3 Ensure Implementation of Board Approved Annual Program and provide required Budget for KYC, AML & CFT Compliance.

7.3.4 Establish and communicate a strong awareness of, and need for effective internal controls, policies and procedures within the organization.

7.4 HEAD OF COMPLIANCE DEPARTMENT SHALL:

The Head of Compliance Department, not below the rank of Manager shall be appointed by the Bank.

7.4.1 Be a member of Assets Laundering Prevention Committee.

7.4.2 Review KYC, AML & CFT Policy prepared by Compliance Officer.

7.4.3 Ensure Implementation of Board Approved Annual Program and Budget for KYC, AML & CFT Compliance.

7.4.4 Have oversight over the KYC/AML/CFT functions.

7.4.5 Report the suspicious transactions in the bank account of nuclear family members or closed family members of Compliance Officer.

7.5 COMPLIANCE OFFICER [CO] SHALL:

The CO not below the rank of Assistant Manager shall be appointed by the Bank to manage the ML & TF risk.

7.5.1 Work as head of KYC/AML/CFT Cell and discharge duty as per roles and duties defined in AML/CFT act, rules and regulator's guidelines.

7.5.2 Work as member secretary of Assets Laundering Prevention Committee (ALPC).

7.5.3 Prepare / Review KYC, AML & CFT Policy and Procedures as per the requirement.

7.5.4 Function as focal point for effective implementation of KYC/AML/CFT policy.

7.5.5 Report to Head of Compliance Department and assist the Head of Compliance in managing the compliance risk. Work as Head of Compliance Department in the absence of Head of Compliance.

7.5.6 Disseminate the FIU, NRB and other investigation authority enquiries to the branches, ensure reply to them and maintain record thereof.

7.5.7 Impart regular training and ensure familiarization of employees with the policy and procedural guidelines.

7.5.8 Monitor financial transactions conducted by customers in the account.

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

7.5.9 Provide Compliance Certificate to PNB and various stakeholders as per the specified frequency.

7.5.10 Prepare risk-based Annual Program and Budget for KYC, AML & CFT after annual risk assessment and recommend to ALPC for review and approval.

7.5.11 Ensure the implementation of Board Approved Annual Program and Budget for KYC, AML & CFT and place the periodical reports to the ALPC for regular monitoring of implementation of Annual Program and Budget for KYC, AML & CFT.

7.5.12 Declare to the Management that he/she has not nuclear family relationship or closed family relationship with the member of the Board or with top management employees of the Regulator i.e. Nepal Rastra Bank.

7.6 PROVINCE MANAGER SHALL:

7.6.1 Act as monitoring level authority and ensure that the bank's policy and procedure relating to KYC/AML/CFT are complied with meticulously in their respective province.

7.6.2 Act as a bridge between the Compliance Department and Branch Designated Compliance Officer so that both Compliance Department employees as well as Branch Designated Compliance Officer can seek support and guidance from respective Province Manager.

7.7 All EMPLOYEES OF THE BANK SHALL:

7.7.1 Read and confirm that they understand the policies and procedures, signing to acknowledge it.

7.7.2 Comply with KYC/AML/CFT policy and procedures.

7.7.3 Remain alert at all times to the possibility of money laundering and reporting suspicious or unusual transactions to the concerned Compliance Officers.

7.7.4 Make effective use of training and seek clarifications whenever necessary.

7.7.5 Be aware that violation of Assets (Money)Laundering Prevention Act &Rules shall attract personal penalties including fines or imprisonment or both and breaches of policy and procedures of the Bank may be construed as gross negligence attracting disciplinary actions as per the Staff Service Byelaws of the Bank.

7.8 INTERNAL AUDIT DEPARTMENT SHALL:

7.8.1 Audit compliance of statutory and regulatory obligations in respect of money laundering policies, procedures and internal controls designed by the Bank.

7.8.2 Audit effectiveness and adequacy of policy, procedure and internal controls designed to counter against the risk of becoming involved in money laundering and terrorist financing by the Bank.

8. COMPLIANCE OFFICER AT VARIOUS LEVELS FOR MANAGING ML & TF RISK

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

The second person in the Head Office Department shall be the Designated Compliance Officer for the Department. Similarly, the second person of the province office shall be the Designated Compliance officer of the province. The Operation In-charge of the Branch shall be the Designated Compliance Officer (BDCO) for the Branch. The Dy. Chief of Rep. Office, New Delhi shall be the Compliance Officer for Rep. Office, New Delhi and Representatives abroad shall also be the Compliance Officer for abroad.

8.1 DEPARTMENT/PROVINCE/BRANCH DESIGNATED COMPLIANCE OFFICER SHALL:

Work as extended arms of HO: Compliance Officer and shall ensure that the bank's policy and procedure relating to KYC/AML/CFT are complied with meticulously.

8.2 COMPLIANCE OFFICER-REP. OFFICE & ABROAD SHALL:

Ensure that the applicable Laws & Regulations consistent with local legal and regulatory/statutory requirements are being complied with.

9. KEY ELEMENTS OF THE POLICY

The key elements of the policy shall be as under:

1. Customer Identification Procedures (CIP)
2. Customer Acceptance Policy (CAP)
3. Customer Transaction Monitoring Procedure (CTMP)
4. Risk Management (RM)
5. Relationship with Customers and others
6. Relationship with Walk in Customers
7. Prohibited Customers
8. Sanctions Screening Policy
9. Risk Based Approach to Customer Due Diligence
10. Periodic Review of Customers profile
11. Record Keeping
12. Reporting of Transactions to FIU/NRB Bank Supervision Department
13. Know Your Employee
14. Confidentiality
15. Code of Conduct for Employee
16. Employee Protection
17. Customer awareness and staff training
18. KYC/AML/CFT Procedure
19. Combating the financing of terrorism
20. Correspondent Banking
21. Wire Transfer
22. Introduction of new technology
23. Resubmission Policy
24. Internal Audit Function
25. Trade Based Money Laundering
26. Performance of ML/TF Risk Assessment and Incorporation thereof

9.1 Customer Identification Procedures

The essence of Customer Identification is to ensure and keep in records the proper identities of the prospective customers/customers and verify the purpose of their intended relationship with the Bank. CIP assists in risk categorization of the accounts and analyzing the deviations

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

in the actual and expected volume and nature of transactions in the accounts to consider if it is suspicious.
A customer's identity shall be verified through reliable documents, i.e. documents issued by Government Authorities. The identification documents include all documents deemed necessary by the Directives of NRB/FIU and the AML/CFT framework of the country. The Customer Name shall be maintained in CBS as mentioned in its identification document without adding any title or salutation or other words. In case of joint account, the name of each individual/venture shall be separated by "/" (slash without prefix or suffix space between the names) only.

Basic information regarding the customers' National Identification Number, addresses, relationships, occupations and sources of income/fund, expected income, expected turnovers/transactions and purpose of establishing a relationship with the Bank needs to be acquired as applicable. The Bank shall maintain the updated list of individuals whose accounts are blocked by the Nepal Rastra Bank or other Law Enforcement Agencies. The Bank shall compulsorily screen such individuals before customer on-boarding and shall not open the account of such individuals whose accounts are blocked by the Nepal Rastra Bank or other Law Enforcement Agencies.

A customer account shall be opened, or business relationships shall be established through electronic means as per the procedural guidelines.

In case, the Government of Nepal has to make government payments including social security, bank shall open the accounts as per the procedural guidelines.

Detailed procedure for Customer Identification Procedures shall be as described in the Procedural Guidelines framed under this Policy.

9.2. Customer Acceptance Policy

The Customer Acceptance Policy ensures that only those clients whose identity and purpose of opening accounts or performing transactions can be duly established and verified as legitimate by conducting due diligence appropriate to their risk profile/services required would be accepted.

For establishing business relationships with new high-risk customers as well as continuing business relationships with existing high-risk customers, approval from Senior Management must be obtained.

The Bank shall have the option to terminate the business relationship with existing customers and close any account if the customer is not providing required documents, details and information for the customer identification and verification and Bank is unable to identify and verify the customers on the basis of documents, details and information made available by the customer. Further, the Suspicious Transaction Report/Suspicious Activity Report relating to business termination due to the above shall be also given to FIU, if necessary.

The Bank shall obtain the thump impression or Bio Metric of account holder and account operator in case of natural person and of account operator in case of legal entity based on the associated risk with the customer at the time of opening the account. But in case of minor, thumb impression or Bio Metric only of account operator shall be obtained.

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

Detailed procedure for the Customer Acceptance Policy shall be as described in the Procedural Guidelines framed under this Policy.

9.3. Customer Transaction Monitoring Procedure

The Customer Transaction Monitoring Procedure (CTMP) is an account/transactions screening mechanism to ensure that the accounts or transactions do have a valid legitimate purpose and by no means are used in money laundering and terrorist financing or any other illegitimate activities. The extent of monitoring of accounts and transactions shall be guided by the degree of risk associated with the accounts/transactions and the anomaly in the transactions with respect to the information disclosed by the customers.

For accounts/transactions that are in the higher risk category or appear to be suspicious, reporting and close monitoring shall be done on a continuous basis.

The Bank shall endeavor to make maximum use of technology and upgrade the systems and procedures to meet the future challenges regarding ML/TF including use of suitable automated Transaction Monitoring System for generation of red flags/alerts in process of identification of suspicious transactions.

9.4. Risk Management

The essence of risk management is to be compliant with the KYC and AML/CFT related Policies, Guidelines and practices. The threats of identity disguise, money laundering and terrorist financing shall be eliminated to the possible extent through effective CDD programs and procedures.

The classification of accounts based on the risk associated with it shall be broadly based on the directions of NRB/FIU. All Customer accounts shall be compulsorily risk categorized under either A (Low Risk), B (Medium Risk) or C (High Risk) Category. The Bank shall further create a sub-risk category under its main risk category (A, B, or C) as required or as defined by the regulatory authority. For example, an 'S' sub-risk under Low Risk 'A' for Simplified Customers, the sub-risk of PEP (Politically Exposed Persons) as defined by NRB under the High Risk “C” Category, and so forth. The Bank shall adopt the risk-based approach for Customer Due Diligence.

Periodic review of customer profile/ information/ document shall be done as per the regulations of NRB/FIU or whenever required. A public notice shall be published at periodic intervals requesting customers to update their account details. Withdrawals in the accounts of customers, whose KYC/updated information, are not maintained due to unavailability of required information from customer within the required time period shall be temporarily restricted. The account shall be revived upon submission of the required KYC documents and KYC verification by the Bank.

Detailed procedure for Risk Management shall be as described in the Procedural Guidelines framed under this Policy.

9.5 Relationship with Customers and others

The Bank shall obtain relevant information as deemed necessary of all its relationship with customers like depositors, borrowers, remittance customers, correspondent banks, remittance agents as well as other associates like consultants, valuators, vendors etc. and shall adopt the following measures:

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

- Obtain KYC documents/information at the time of commencing of business relationship.
- Strictly follow the customer identification procedures and customer acceptance policy, which are basic elements of KYC.
- Carry out initial Due Diligence at the time of establishing a relationship. This shall include, but not limited to, the verification of antecedents and screening procedures to verify that the customer has a clean history/business record and any family relationship with politically exposed person (PEPs).
- Comply with Anti-Bribery and Corruption law/provisions of the country.

9.6 Relationship with Walk in Customers

The Bank shall obtain the KYC documents and identify the Walk in Customers in case of transactions of rupees one lac or more (including foreign currency transactions equivalent to rupees one lakh or more). Likewise, in case of cash deposit or cash withdrawal of above rupees one lakh or equivalent by other than account holder, bank shall obtain Identity documents of cash depositing or cash withdrawing person and reason for depositing cash or withdrawal. However, obtaining identification documents issued by Government Agency having customer photo, issued date, issued place or expiry date (if applicable) of cash depositing or cash withdrawing person shall be preferred for reliability of Identity documents.

9.7 Prohibited Customers/Products & Services

The Bank shall not open an account of the following customers or establish a business relationship or conduct transactions with such customers:

- Anonymous or Fictitious Accounts
- Shell Entities i.e. Shell Banks/Shell Companies
- Entities (including natural person, legal person, etc.) sanctioned by major sanction authorities such as United Nations, Office of Foreign Assets Control (OFAC)-USA, Her Majesty's Treasury (HMT)-United Kingdom, European Union, Ministry of Home Affairs, Nepal (MOHA), etc.
- Sanctioned Countries
- Offshore Banks
- Downstream correspondent Banking
- Payable through accounts
- Customers from Jurisdictions subject to a FATF call on its members and other jurisdictions to apply countermeasures (presently: Democratic People's Republic of Korea (North Korea) and Iran) [Source (FATF Website): https://www.fatf-gafi.org/]
- Customers not providing required documents, details and information for customer identification and verification.
- The bank is unable to identify and verify the customers based on available documents, details and information.
- Unlicensed/Unregulated Banks and Financial Institutions, Payment system operator and provider, Non-Financial Institutions, remittance agents, exchange houses or money transfer agents.
- Red light business/ Adult entertainment
- Marijuana/illegal drugs
- Gambling
- Blacklisted Person, firm, company and organizations etc.
- Unregistered and unregulated charities
- Bit coin / Crypto Currency/ Digital/ Virtual Currency.

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

- Arms, Defense, Military (Except Government approved)
- Atomic Power (Except Government approved)
- Regulatory blocked person, firm company and organization

However, the following customers shall be subject to ECDD:

- Jurisdiction subject to a FATF call on its members and other jurisdictions to apply enhanced due diligence measures proportionate to the risks arising from the jurisdiction ensuring UN targeted and sector specific sanctions, US-OFAC, UK-HMT, EU & sanction list published by Government of Nepal, Ministry of Home Affairs (MOHA) are meticulously complied with. [Source (FATF Website): https://www.fatf-gafi.org/]
- Customers from FATF Jurisdictions under Increased Monitoring
- Tax Haven Countries
- Highly Corrupt countries based on Transparency International Corruption Perception Index (CPI)
- High Risk Customers

The list of High-Risk Countries including Sanctioned Countries, FATF-High Risk Jurisdictions-Call for action, Jurisdictions under Increased Monitoring, Tax Heaven Countries and Highly Corrupt countries shall be provided by the Compliance Department to the branches

The CEO may waive the restriction on prohibited customers, countries, products, and services on a case-to-case basis after applying enhanced due diligence measures proportionate to the risks arising from it, ensuring meticulous compliance with UN targeted and sector-specific sanctions, US-OFAC, UK-HMT, EU, and the sanction list published by the Government of Nepal, Ministry of Home Affairs (MOHA).

The above list is indicative only and not exhaustive.

9.8 Sanctions Screening Policy

Sanctions screening is a common global challenge facing banks and financial institutions. Any person or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the Targeted Financial Sanctions as per United Nations Security Council Resolutions (UNSCR) 1267 (1999) and 1373 (2001) and its successor resolutions and prevention and disruption of the financing of proliferation of WMD as per United Nations Security Council Resolutions (UNSCR) 1540 (April 2004) and its successor resolutions shall be screened and such listed person/entity asset/fund, held singly or in joint ownership, increment in such fund/asset shall be freezed without delay and reported to Money Laundering Prevention Supervision Department, Nepal Rastra Bank and FIU- Nepal within 3 days from the freeze date as per the provisions contained in the Section 29 (Chha) of Asset (Money) Laundering Prevention Act 2064 as per Annexure 10 of Asset (Money) Laundering Prevention Rules 2081.

Bank shall have an appropriate Sanction Screening mechanism whereby the required sanction lists such as US OFAC, UN, EU, UK HMT, PEP list, enforcement list, adverse media list, bank's internal watch list or any other sanctions list whenever gets updated shall be reflected immediately and branches/departments shall be able to do the real time screening at the time of customer on boarding and cross border transactions. Similarly, a batch

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

screening shall be carried out of the entire existing customer against the updated list periodically.

The branches or any other suitable unit defined in the procedure must ensure that no accounts are allowed to be opened in the name of sanctioned entities and individuals appearing in the sanction list besides transactions with them.

The BDCO in the Branch shall invariably check all account opening requests against the above referred lists and must certify having checked and no match found on the account opening form.

9.9 Risk Based Approach to Customer Due Diligence

Keeping in view the large volume of customers and transactions, the bank shall focus on the areas where risks are relatively high by adopting the risk-based approach so as to allocate resources in the most effective way. The bank shall carry out the due diligence of the customer based on the risk. The Bank shall conduct simplified Customer Due Diligence (SCDD) for Low-risk customers having annual transactions of rupees one lac and below. The Bank shall conduct Customer Due Diligence (CDD) for all other Low risk customers and Medium Risk Customers. The Bank shall conduct Enhanced Customer Due Diligence (ECDD) for High-Risk customers. However, the risk category shall be dynamic as it shall be updated as per the changed profile of the customers and activities in their accounts.

In addition to the above, risk profiling shall be done on different grounds such as country or geographical area, business/profession, customer, products / services and delivery channel etc. or as required by related Acts and NRB/FIU Directives.

9.10 Periodic Review of Customers profile (KYC Renewal)

The bank shall conduct an on-going due diligence to effectively control and reduce the risk from customers. The bank shall pay more attention to the transactions that do not match with the customer profile, line of business, high value transactions, high account turnover and transactions exceeding threshold limit. The Bank shall conduct periodic reviews of customers i.e., Customer Due Diligence (CDD) for Low-risk customers every eight years and Medium Risk Customer every five years. Similarly, the Bank shall conduct Enhanced Customer Due Diligence (ECDD) for High-risk customers annually or as per the requirement. However, customers in all risk categories shall be reviewed immediately upon any trigger events or in case of any unusual activities/deviation from the customer profile are observed.

9.11 Record Keeping

All documents and other information related to the identification and verification of customer and beneficial owner, and documents and records related to domestic and foreign transaction with the client and or beneficial owner and records pertaining to account opening must be preserved at least 5 years from the date of cessation of the transaction with the client. The identification records and transaction data should be made available to the Law Enforcement Agencies upon request. The Bank shall keep the report of suspicious transactions for 5 years.

However, in the case of PEPs and PIPs it is required to safely keep the record for at least ten (10) years from the date of separation from his/her position. For this, the branches shall obtain the information in the Customer Information Form (CIF) at the time of opening of their new account or during the periodic review of their account.

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

Bank shall maintain the records of customer and its beneficial owner via electronic media so that it can be checked and analyzed as per the requirement at any time or for submitting to the regulator in a prescribed format.
Bank shall update fundamental information, details and documents of customer and individuals including of beneficial owner based on inherent risk regularly through electronic technology. For this purpose, banks shall develop and implement information technology portals.

9.12 Reporting of Transactions to FIU/NRB Bank Supervision Department

The Compliance Officer shall report regarding the following:

A. Through SIS Reporting Portal

a. Revised KYC/AML/CFT Policy, KYC/AML/CFT Procedure and KYC/AML/CFT Annual Budget and Planning at least once in a fiscal year.

b. The Annual Report regarding the activities of the Bank implied and achieved during the last fiscal year regarding Anti Money Laundering, Combating Financing on Terrorist Activities and Proliferation Financing within 2 months following the fiscal year end.

c. The AML CFT Reporting Form (NRB 14 SIS XBRL Report) shall be prepared and submitted semi-annually.

B. NRB, Money Laundering Prevention Supervision Division, FIU-Nepal and Non-banking Supervision Department

a. Appointment of Compliance Officer or updating the change information regarding the Compliance Officer through goAML (Production Environment)

b. A0002 – Report for AML/CFT as per schedule no.19.2 of NRB Directives Chapter 19 within 15 days from each quarter end.

C. NRB, Money Laundering Prevention Supervision Division and FIU-Nepal

a. The AML CFT Reporting Format (Offsite Data Collection Form) on a half yearly basis.

b. The AML CFT Reporting Format (Bank's Self-Assessment Questionnaire) on a yearly

c. The risk assessment of the bank pertaining to ML/TF risk annually within first quarter of each fiscal year after the approval of ALPC and the Board.

However, prior to the annual ML/TF risk assessment, the Bank shall submit the assessment methodology and format to NRB, Money Laundering Prevention Supervision Department.

D. FIU-Nepal

a. Threshold Transaction Reports (TTRs): Reports of the following transactions one time or in a series in a day as per prescribed threshold limits will be made within 15 days from the date of transactions:
   1. Cash Deposit or withdrawal
   2. Inward or outward remittance (cross border transactions)
   3. Exchange of foreign currency
   4. Any other defined by the Regulator

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

b. Suspicious Transaction/ Activity Reports (STRs / SARs): The report on suspicious transactions / activities would be made immediately after reaching the conclusion that the transaction / activity is of suspicious nature. Suspicious transactions/ activities shall also include an attempted transaction, whether made in cash or not irrespective of the transaction amount. STR/SAR are submitted to FIU Nepal only from Compliance Department through goAML software as per the goAML Schema under goAML Operational Guidelines and Suspicious Transaction Reporting & Suspicious Activity Reporting (STR/SAR) Guidelines issued by FIU Nepal in July 2021 or its amendments from time to time.

During the process of identifying suspicious transactions, if the Bank believes that informing the customer for KYC updates, verification, or further due diligence of the transactions shall compromise the suspicious reporting process, it shall be conducted these activities only after reporting the suspicious transactions to FIU Nepal.

E. Other Reports as and when required by the Regulators

Detailed procedure for reporting TTR/STR/SAR and other reports shall be as described in the Procedural Guidelines framed under this Policy.

9.13 Know Your Employee

Know Your Employee (KYE) standards shall be defined and implemented by the HR Department from time to time to ensure that unwanted individuals do not have access to the Bank by way of employment. The HR Department shall screen the potential employees prior to new appointments and periodically the existing staff through the Compliance Department. Head-HR shall ensure that any prima facie suspicious activity of employee from the AML/CFT angle is reported to Compliance Officer for finalization and reporting to FIU (NRB).

The newly recruited and promoted staffs (including Top Management, Heads of Departments (HOD), Province Managers (RM), Branch Managers (BM), and all other permanent and contract staff) are required to submit their updated KYC details. These details should include their new annual income scale, account turnover, staff position, number of transactions, etc. This must be done within one month of the recruitment date for new staff, and within three months of the effective promotion date for promoted staff. The information should be submitted to the respective branches where their staff accounts are maintained. Failing to update KYC, the account of the concerned staff shall be debit frozen.

9.14 Confidentiality

The Bank shall keep the details of all transactions of STRs, TTRs and correspondence records to and from FIU, NRB and other investigation bodies relating to its customers under the investigation strictly confidential and shall not share the same with the customer or any irrelevant bank staffs, unrelated official meetings or anyone outside the bank. The bank shall keep the documents, information and transaction details of the customer confidential and shall not leak/share to unauthorized person.

9.15 Employee Protection

The bank shall not take any action to reporting staff, BDCO, DDCO, Head-Compliance and Compliance Officer in case any loss occurs to a customer or bank's business due to submission of information to the FIU or other investigation agencies as per section 37 of AMLP Act 2064 (2nd amendment 2070) which states "No Criminal, Civil, Disciplinary or Administrative action or Sanction shall be taken against a government agency, reporting entity or any of their

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

official or staff who in good faith submit reports or provide report, document, information, notice or records in accordance with the provisions of AMLP Act 2064, AMLP Rules 2073 and directives issued there under as a breach of secrecy provision under prevailing laws or contractual, administrative or regulatory liability.

The bank shall bear the full legal expenses and protect its employees if a legal case is filed by the customer against any staff, BDCO, DDCO, Head-Compliance and Compliance Officer.

9.16 Code of Conduct for Board of Directors, Chief Executive Officer and Employees

The Board of Directors, Chief Executive Officer and employees will conduct themselves in accordance with the highest ethical standards and the extant regulatory requirements and laws. The Board of Directors, Chief Executive Officer and Employees should not provide advice or other assistance to individuals who are indulging in money laundering / terrorist activities. Any knowledge / information of the Board of Directors, Chief Executive Officer and Employees involved in such activities shall not be kept hidden and shall be escalated to the compliance officer/higher authorities. The Board of Directors / Management shall provide adequate safeguards to whistle blowers including the anonymity of the whistle blower.

1. The Bank employees filing suspicious reports must not tip off. He/she needs to maintain the following code of conduct:
   - Must not inform/warn the customer about the suspicion.
   - Must not talk/disclose with other staff or friends or family members.
   - Must comply with the instructions of Compliance Officer to which he/she reports.
   - Must assist and cooperate with the Compliance Officer during the investigation process.

2. The code of conduct has three aspects:
   - Relationship with the customer should not be damaged / disturbed if the authorities recognize the transaction to be bona fide.
   - If a customer or his/her transaction is identified as money laundering or a part of its process, the authority will be in a better position to arrest him/her and there will be less chance of erosion of evidence.
   - The Board of Directors, Chief Executive Officer and Employees failing to report suspicious transactions and suspicious activity will be held liable for punishments i.e. legal and/or disciplinary actions.

The Board of Directors, Chief Executive Officer and employees shall keep the information relating to its customers under the investigation strictly confidential and shall not share the same with the customer or any irrelevant bank staffs, unrelated official meetings or anyone outside the bank.

9.17 Customer Education and Staff Training

The Bank recognizes the need to spread awareness on KYC, Anti Money Laundering measures and Terrorist Financing and the rationale behind them amongst the customers and shall take suitable steps for the said purpose. The customer awareness materials on KYC/AML measures will be displayed on the bank's website and in the form of poster/display boards, etc.

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

Compliance Department shall assist in conducting general and specific KYC/AML/CFT trainings/seminars through class room or online mode at regular intervals through-out the year at various Centers as per yearly/quarterly training calendar prepared by the HR Department, so that necessary and regular awareness in regard to Bank's obligations under AMLPA, 2064 as well as NRB/FIU guidelines are disseminated to all levels of Bank's functionaries especially Customers Service Staffs, BDCO and Branch Managers who have been vested with the responsibility of ensuring meticulous compliance with KYC/AML/CFT Regulations. Besides, training and education will be imparted to staffs members whenever any new issues occur in the market e.g. significant regulatory actions or new regulations. The record of the training shall be maintained by the HR Department as well as the Compliance Department.

A Knowledge sharing program on KYC/AML/CFT compliance for the Shareholders holding 2% and above shares, Board Members and Senior Executives shall be conducted through classroom or online mode at least annually for the qualitative enhancement of corporate governance and risk management system.

9.18 KYC/AML/CFT Procedures

A separate KYC/AML/CFT procedural guideline prepared by the Compliance Department with the approval of the CEO shall supplement this policy for effective implementation of the provisions of this policy. The existing KYC/AML/CFT procedure and internal circulars issued by the Bank shall prevail until the revision of KYC/AML/CFT procedures.

9.19 Combating the Financing of Terrorism

The Section 18(9) of NRB Unified Directives 19/2078 requires Banks to make provisions for prevention of Terrorist Financing (TF) activities and financing of production and proliferation of weapons of mass destruction. Further, it also requires Banks to develop mechanism for identification, monitoring and reporting on TF activities and financing of production and proliferation of weapons of mass destruction.

Further, the UNSCR 1267 (1999), UNSCR 1373 (2001) and its successor resolutions require countries to immediately freeze funds, financial assets or economic resources of individuals and entities who are designated by the United Nations Security Council based on such person's / entity's connections with terrorism and terrorist financing. Further, countries should ensure that no funds, financial assets or economic resources are made available to or for the benefit of such designated persons or entities or their beneficiaries. The updated list of such individuals/entities can be accessed from the sanction detail uploaded on bank's intranet and from the United Nations website at https://www.un.org/securitycouncil/content/un-sc-consolidated-list.

Branches/Offices before opening any new account must ensure that the name(s) of the proposed customer does not appear in the list.

The Branches/Compliance Department shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. The branches shall immediately freeze funds or assets of such individuals/entities in case of any accounts bearing resemblance with any of the individuals/entities in the list and shall immediately intimate to Compliance Officer, Head Office for onward submission of the same to FIU, NRB.

9.20 Correspondent Banking

CONFIDENTIAL FOR INTERNAL CIRCULATION ONLY

This policy shall apply to our dealings with correspondent banks. For correspondent banking relationship, sufficient information shall be obtained to understand the nature of their business activities, ownership structure, Management details, PEPs and RCAs screening, social media search shall be done to verify the publicly available information. Further, an appropriate due diligence procedure will be laid down keeping in view KYC standards existing in the country where the correspondent bank is located and the track record of the correspondent bank in the fight against money laundering and terrorist financing. The Bank's Remittance Department and Treasury Department, Head Office shall conduct CDD/ECDD for the Bank's existing correspondent banks on an annual basis in the format prescribed by the Bank. Before establishing a correspondent banking relationship, approval from senior management must be obtained.

9.21 Wire Transfer

All wire transfers shall include meaningful originator information (name, account number or transaction ID, address or birth date and birthplace or citizenship number or national id number or customer id number, Beneficiary Name and Account Number or transaction ID and/or account number) and to conduct enhanced scrutiny of monitoring for suspicious activity where originator information is not provided. Originator means the beneficial owner remitting the fund through wire transfer. The Bank shall ensure the complete information of sender and beneficiary in the wire transfer message before initiating the transaction and the information remains with the wire transfer or related message throughout the payment chain. Similarly, the transfer of fund should be in line with the customer's business profile. The above provision shall be applicable in case of wire transfer through batch file also.

For carrying cross border correspondence banking transaction smoothly by making risk free, bank shall fulfil national and international values and norms related with correspondence banking i.e., FATF recommendation 16, Wolfsberg Group Payment Transparency standards and local regulations. The Bank will respond to Request for Information (RFI) from other entities in a timely manner and similarly ask for missing information and details from other entities also.

Branches/Department shall ensure that, in the context of processing wire transfers, take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), relating to the prevention and suppression of terrorism and terrorist financing.

9.22 Introduction of New Technology

Bank will pay special attention to the money laundering threats arising from existing, new or developing technologies and take necessary steps to prevent its misuse for money laundering activities. The Bank will ensure that appropriate KYC procedures are duly applied to the customers using new technology-driven products and while initiating non-face to face customer services or transactions.

The bank shall deliberate, assess and review details of the procedural arrangement required for mitigating ML/FT risk during the development of new product paper or while introducing the new delivery channel in the Bank or any amendment thereon.

9.23 Resubmission Policy

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

Once a transaction is rejected due to sanctions/money laundering/terrorist financing concerns, the concerned department/branches shall maintain the record of such rejected transactions and shall not attempt to resubmit the same transaction after stripping off and or masking of information as well as ensure that the transactions rejected by correspondent bank are not re-submitted.

However, if a transaction is rejected due to the ML/TF risk appetite of one correspondent bank, it shall be resubmitted through another correspondent bank without stripping off and/or masking the information. Such transactions are considered high risk, require enhanced due diligence, and need Senior Management Approval for resubmission after proper verification and sanction screening.

9.24 Internal Audit Function

The Bank shall maintain an independent audit function (Internal Audit Department) that is adequately resourced and able to regularly assess the effectiveness of the banks internal policies, procedures and controls and its compliance with regulatory requirements especially covering the aspect of KYC/AML/CFT issues and shall have a separate section under Operations Section in its audit report of the branches.

The Internal Audit Department shall provide the consolidated KYC/AML/CFT compliance report annually to Audit Committee Board (ACB) on the basis of its audit findings in the branches during the fiscal year.

9.25 Trade Based Money Laundering

Trade Based Money Laundering (TBML) is the process of disguising the proceeds of crime and moving money through the use of trade transactions in an attempt to legitimize their illicit origins. Such activities are done through over- and under-invoicing of goods and services, multiple invoicing of goods and services, over- and under-shipments of goods and services, and falsely describing goods and services. All the trade transactions shall be strictly screened against the sanctions and verified prior to the execution and ensure that the customer due diligence is carried out and required documents are obtained as per the prevailing NRB's guidelines/regulations. The bank before processing the import instruments (LC/TT/DD/DAP/DAA) shall obtain the proforma invoice from the customer and scrutinize/ensure the content and price mentioned in the proforma invoice is in line with the mandatory provisions stipulated by the Nepal Rastra Bank Directives/Circulars.

9.26 Performance of ML/TF Risk Assessment and Incorporation thereof

The Bank on an annual basis shall perform the ML/TF Risk Assessment of the Bank for the financial year within the 1st quarter from the end of financial year.

The risk assessment process shall include the following:

- Identify the material and foreseeable ML/TF risk and vulnerabilities which the bank is exposed to during the business.
- Determine the level of ML/TF risk involved for each group or type of customers, business relationships, product or services, delivery channel and geographical location offered by financial institutions within its business;
- Document the risk assessment.
- Submit risk assessment to NRB within stipulated time through stipulated process after review from the Board;

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

- Formulate policies, procedures and control measures to mitigate and manage the identified risk in an effective manner.
- Must be used to develop AML/CFT program.
- Monitor the implementations of the control measures adopted and enhance the measures regularly; and
- Identify deficiencies; make necessary changes and review to ensure it is up to date.
- Audit of risk assessment by Internal Audit to assess its adequacy and effectiveness.

The bank may establish a manual or automated system to perform its risk assessment.

The Bank shall evaluate the likelihood and extent of its ML/TF risks at a macro level. While assessing the ML/TF risks, the Bank will consider all relevant risk factors that affect their business and operations, which may include the following:

a) Type of customers;
b) Geographic location;
c) Transactions and distribution channels offered by the reporting institution;
d) Products and services offered by the reporting institution;
e) Structure of the reporting institution; and
f) Findings of the National Risk Assessment (NRA), Mutual Evaluation Report, AML/CFT National Strategy, typologies envisaged by FIU (through guidelines or annual reports) and guidelines issued by the NRB.
g) Methods and trends used for ML/TF (also called typologies) published in the FATF, APG and other AML/CFT agencies report.
h) Other factors such as filed STRs/SARs typologies, emerging trends and typologies in the banking sector in relation to ML/TF risk, internal audit and regulatory findings.

The findings of the above AML/CFT risk assessment shall be incorporated into the KYC/AML/CFT Procedure of the Bank immediately after approval of the KYC/AML/CFT Policy from the Board.

9.27 Credit Client Policy

While analyzing the credit proposals, accepting credit client or continuing the business relationship with existing credit client, the Bank shall strictly comply with the AML/CFT provisions laid down under this policy.

The Bank shall perform thorough background checks and verification processes for loan customers, especially for high-value loans. This includes understanding the borrower's financial history, source of income, and creditworthiness.

The recommending officials and sanctioning committees shall scrutinize loan applications for any signs of suspicious activity. This could involve verifying the legitimacy of the stated purpose of the loan, cross-referencing information provided by the customer, ensuring the loan amount aligns with the customer's financial profile, and verifying the legitimacy and value of any collateral or guarantees provided by the borrower to prevent fraudulent activities.

The branches and/or HO Monitoring Unit shall continuously monitor how loan funds are disbursed and used. This includes ensuring that the funds are used for the stated purpose and not diverted to illicit activities. The branches shall keep an eye on loan repayments to detect any irregular patterns or discrepancies. It is confirmed that the source of the borrower's

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY

funds, especially if large amounts are involved, doesn't come from illegal activities. The sudden large repayments or repayments from unknown sources are closely monitored and if any suspicious activities are detected during the loan process, post loan sanctions or during settlement, promptly report them to the Compliance Department. This may include filing Suspicious Transaction Reports (STRs) or Suspicious Activity Reports (SARs) to FIU-Nepal, if necessary.

The branch shall conduct regular reviews and updates of the loan customers' profiles, especially if there are significant changes in their financial situation or behavior.

10. REPORTING & MONITORING MECHANISM

10.1 REPORTING MECHANISM

10.1.1 REPORTING TO FIU

The Compliance Department shall ensure the timely reporting to FIU enquiries by obtaining the information from the Branches / Departments. The Branches / Departments shall provide the sought information to Compliance Department within specified time frame from the receipt of the correspondence from the Compliance Department.

10.1.2 REPORTING TO OTHER INVESTIGATION AGENCIES

The Compliance Department/Branches shall ensure the timely reporting and information to other investigation agencies enquiries. The Compliance Department / Branches shall provide the sought information to investigation agencies within stipulated time period. The Branches shall provide the information to investigation agencies under intimation to Compliance Department.

10.1.3 REPORTING TO MANAGEMENT, ALPC AND BOARD

The Compliance Department/CO shall report monthly or as per the requirement regarding KYC/AML/CFT status to Management. Compliance Department/CO shall report quarterly or as per the requirement regarding KYC/AML/CFT status to ALPC and Board.

If any action is initiated against the Bank due to delay/wrong confirmation in the sought information to FIU, NRB and other investigation agencies, the designated staff of the branches/departments shall be held accountable, and the action shall be taken as per the bank's staff service byelaws.

10.2 MONITORING SYSTEM

10.2.1 Periodical monitoring of KYC Norms, AML & CFT measures shall be done by the various compliance functions.

11. RISK APPETITE AND TOLERANCE

The Bank shall pursue a zero-risk appetite & tolerance on all matters related to AML/CFT compliance.

12. MISCELLANEOUS

Information collected from the customers for KYC compliance should be relevant to the perceived risk and not intrusive and not used for cross-selling.

- Information like citizenship cards, residential proof etc. already obtained at the time of opening of an account shall not be asked at the time of updating of KYC and periodic

CONFIDENTIAL- FOR INTERNAL CIRCULATION ONLY

review of account. The branches shall obtain only the changed information and other required documents and may obtain additional documents based on inherent risks associated with the customer.

- Bank may obtain the required documents for identification of customer and beneficial owner from any suitable media other than the details which required to be submitted by the customer presenting himself.

- For identifying/reviewing corporate customers, the bank may obtain the latest audited financials if deemed necessary as per the inherent risk associated with the customer.

- Bank shall not apply same identification procedure to all types of customers and beneficial owner but required to adopt risk-based approach.

- Banks are required to do ECDD of the customer of high-risk country on the basis of corruption, tax evasion or on the basis of place where the customer is residing or doing business, It is also required to do ECDD while establishing business relations and carrying transactions with the customer that carry transaction only through electronic media.

- The bank shall not issue any negotiable bearer instruments. Any cross-border remittance of funds by way of demand drafts, speed remittance, RTGS, SWIFT transfer needs to be affected only by debit to customer's account and not against cash.

- Branches should also note that suspicious activity reports are required to be filed even in respect of attempted / abandoned transactions, unscrupulous enquiries by individuals and forfeiture of activities / transactions after enquiries are made.

13. REVIEW OF THE POLICY

The Policy shall be reviewed at least once in a fiscal year to incorporate the amendments in existing laws, results from the Bank's Annual Risk Assessment for ML/TF, change in business or technology, emerging trends and new methods of conducting financial crime or as and when required. The policy shall come into effect from the Board approval date and shall remain effective till the next review takes place. Once approved by the Board, the policy shall be communicated to all branches and made available on the bank's intranet (i.e. Infocenter).

14. SUPERSEDES

To implement the changes in Acts or direction, immediately upon issuance Supersedes
If there are any changes/addition in the regulations, acts, or directives from the Central Bank (NRB) or the Government of Nepal (GoN) regarding AML/CFT issues, the provision of new regulations, acts, or directives, will automatically added to the policy or supersede the existing provision of the policy.

15. REPEAL & SAVINGS

This policy shall come into force upon approval by the Board and shall substitute earlier policy. All actions taken and functions performed before the commencement of this policy shall be considered to have been taken or performed pursuant to this policy.

CONFIDENTIAL - FOR INTERNAL CIRCULATION ONLY