NMB BANK LIMITED
एनएमबि बैंक लिमिटेड
("A" class commercial bank licensed by Nepal Rastra Bank.)

Bank of the Year, ASIA 2021
Bank of the Year, Nepal
2017, 2018, 2020 & 2021

NMB Group

Anti-Money Laundering and Combating Financing of Terrorism Policy

Version 2

NMB Bank Limited
July 2025

Revision History & Version Control

Sn	Version	Approving Authority	Date of Approval
1	1st	387nd Board Meeting	25th July 2019
2	2nd	497th Board Meeting	10th October 2025

Information Sheet

Target Audience:
All the businesses carried out by NMB Group Entities and Group staffs.

Issued By:

NMB Bank Limited

Replaces:
Version 1

Valid From:
Immediately after Board Approval

Document Classification: Internal

Table of Contents

Acronyms

ALPA	Asset (Money) Laundering Prevention Act
ALPC	Assets Laundering Prevention Committee
AML	Anti-Money Laundering
AMLPO	Assistant Money Laundering Preventions Officer
CBS	Core Banking System
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CFT	Combating the Financing of Terrorism
DCEO	Deputy Chief Executive Officer
ECDD	Enhanced Customer Due Diligence
FATF	Financial Action Task Force
KYC	Know Your Customer
ML	Money Laundering
MLPO	Money Laundering Preventions Officer
NRB	Nepal Rastra Bank
PEP	Politically Exposed Person
PF	Proliferation Financing
RMC	Risk Management Committee
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorist Financing
WMD	Weapons of Mass Destruction

1. Introduction

The NMB Bank Group consisting of NMB Bank Ltd, NMB Capital Ltd., NMB Laghubitta Bittiya Sanstha Limited. and NMB Securities Ltd, places greater emphasis on integrity and good governance and is committed to the highest standards of anti-money laundering and combating the financing of terrorism in line with the principles and standards of applicable legislation. best banking practices and applicable market standards including, where relevant, other international financial institutions' standards.

2. Scope

This "NMB Group Anti-Money Laundering and Combating Financing of Terrorism Policy" establishes the key principles regulating AML-CFT and related integrity aspects in NMB Bank Ltd., NMB Capital Ltd., NMB Laghubitta Bittiya Sanstha Limited. and NMB Securities Ltd. for their respective daily operations.
Adherence to the policy and its implementing procedures is the shared responsibility of all NMB Group staff and members of governing bodies.

2.1 Objectives

The standards set out in this policy are minimum requirements based on applicable legal and regulatory requirements and apply to the entire NMB Group. These requirements are intended to prevent NMB Group, our employees and clients from being misused for money laundering, terrorism financing, proliferation financing or other financial crime. This Policy establishes the general framework for the fight against money laundering and financing of terrorism and proliferation.

2.2 Applicability

Sub-section 1 of section 7 Tha of the Asset (Money) Laundering Prevention Act. 2008 (as amended from time to time) imposes duty on NMB Bank Ltd to ensure that the legal duties resulting from the regulations set out in this Act and the Directive No 19 of Unified Directive issued by Nepal Rastra Bank are fulfilled by our subsidiaries in Nepal and abroad as well.

Similarly, sub-section 2 of section 7 Tha of ALPA, 2008 (as amended from time to time) imposes duty on NMB Bank Ltd to prepare and implement Group AML-CFT policy and procedure. Wherever subsidiaries' AML/CFT policies are more stringent than the requirements set out in this Policy, the stringent standard shall be applied.

2.3 Definitions

Money Laundering

Money Laundering is an activity involving transaction/or series or transactions that is designed to disguise the nature/source of proceeds derived from illegal activities, as defined in the (Money) Laundering Prevention Act, 2008 (as amended from time to time), which may comprise drug trafficking, terrorism, organized crimes. murders, fraud. etc

It is important for all employees of the Group to be conversant and familiar with the ML process (described below) as they must be vigilant all the times and should any of the aspects involved in ML process surface in our business they must be able to identify the warnings sign and take appropriate actions.

Stages of Money Laundering:

Placement: The first stage of ML is successfully disposing of the physical cash received through illegal activity. The criminals accomplish this by placing this into a financial institution. During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos and other legitimate businesses, both domestic and international.

Examples of placement transactions include the following:

- Blending of funds: Commingling of illegitimate funds with legitimate funds, such as placing the cash from illegal narcotics sales into cash-intensive, locally owned restaurant
- Foreign exchange: Purchasing of foreign exchange with illegal funds
- Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade reporting requirements
- Currency smuggling: Cross-border physical movement of cash or monetary instruments
- Loans: Repayment of legitimate loans using laundered cash

Layering: The second stage concentrates on separation of proceeds from criminal activity through the use of various layers of monetary transactions, intended to conceal the origin of the proceeds. These layers are aimed at wiping audit trails, disguise the origin and maintain anonymity for people behind the transaction.

Examples of layering transactions include:

- electronically moving funds from one country to another and dividing them into advanced financial options and/or markets;
- moving funds from one financial institution to another or within accounts at the same institution;
- converting the cash placed into monetary instruments;
- reselling high-value goods and prepaid access/stored value products;
- investing in real estate and other legitimate businesses;
- placing money in stocks, bonds or life insurance products; and
- using shell companies to obscure the ultimate beneficial owner and assets.

Integration: The final link in ML process is sometimes called the integration stage. This occurs when the laundered or cleaned up money is legitimately brought back into financial systems operated by end user and when it is safe and insulated from enquiry by any agency for a legitimate reason for querying the existence of money.

Examples of integration transactions include:

- purchasing luxury assets, such as property, artwork, jewelry or high-end automobiles; and
- getting into financial arrangements or other ventures where investments can be made in business enterprises.

These "stages" are not static and overlap broadly. Financial institutions may be misused at any point in the Money laundering process.

Terrorist Financing

Terrorist financing provides funds for terrorist activity. The main objective of terrorist activity is to cause substantial damage to property/human; or seriously interfering with or disrupting essential services, facilities or systems.

There are two main sources of terrorist financing – financial support from countries, organizations or individuals, and revenue-generating activities that may include criminal activities. The second source, revenue generating activities, may involve drug trafficking, human smuggling, theft, robbery and fraud to generate money. Funds raised to finance terrorism usually have to be laundered and thus anti-money laundering processes in banks and other reporting industries are important in the identification and tracking of terrorist financing activities.

Bank shall build measures to monitor, identify and report such funds received or sent using the banks system. Bank shall take caution while doing transaction, account opening or carrying banking activities if in any circumstances the name of any banned organization or individual (involved in terrorist activities) appears as payee/endorsee/applicant and report of such transaction as and when detected.

The Bank shall endeavor to get the list of such organization/individuals to the best possible means or mechanisms.

Proliferation Financing

Proliferation financing (PF) refers to the financial support provided for acquiring, developing, or exporting WMDs, including nuclear, biological, and chemical weapons. It remains a global concern, with international bodies such as the United Nations (UN) and FATF enforcing strict measures to curb these activities. Nepal, though distant from global proliferation concerns, must continue strengthening safeguards to prevent any misuse of its financial system for proliferation financing purposes.

Mitigating proliferation risk involves international cooperation, robust regulatory frameworks, intelligence sharing, and effective enforcement measures to prevent the spread of WMD and ensure global security.

Bank shall conduct CDD measures to assess the background of clients and the nature of client's business and its potential involvement in sectors that may be associated with WMD development. Bank shall also establish systems to monitor transactions for unusual patterns or activities that may indicate proliferation financing, such as large cash transactions, transfers to high-risk jurisdictions, or transactions involving dual-use goods.

The bank shall regularly screen clients and transactions against national and international sanctions lists related to proliferation, such as those maintained by the United Nations (UN), United Kingdom (UK), the European Union, and the U.S. Office of Foreign Assets Control (OFAC).

3.Minimum Requirements

All NMB Bank and subsidiaries have to comply with the following basic principles:

a. Ascertainment of Customer Identity:

- When entering into a business relationship,
- When performing a single transaction or deal
- Urgent transactions exceeding prescribed limit.
- Electronic Wire Transfers.
- Every transaction by High Risk Customers or High-Level Officials.
- As advised by Regulators.

Group entities must exchange information on measures taken to identify customers and combat risks associated with AML-CFT in case of occurrence of ML activities.

b. Establishment of Purpose of Business Relationship:

When entering into a business relationship, NMB Group must obtain information on kind and purpose thereof, if this is not clear from the business relationship itself.

c. Identification of Ultimate Beneficial Owner:

Whenever NMB Group is required to identify a customer, it must establish and verify the identity of the ultimate natural person;

- who owns or
- controls the customer or its assets or
- on whose behalf' the transaction is carried out or the business relationship is established

d. Client Account Monitoring:

A permanent monitoring of clients' accounts must be implemented to detect unusual/suspicious transactions and report STR/SAR. Monitoring must be conducted for applicable business areas using adequate processes and systems.

e. Correspondent Banking:

Special attention must be paid to correspondent banking business and adequate security measures must be implemented.

f. Forbidden Business:

Payable through accounts and relationships with shell banks are forbidden.

g. Reporting of Suspicious Circumstances/Transactions:

Such circumstances/transactions must be reported to the competent authorities according to local law. The Group entities must ensure that the exchanged information are kept confidential.

h. Staff Reliability:

NMB Group shall screen the staff details on AML perspective (criminal activities, sanction list etc.) before recruitment of staff. It is also applicable for outsourced staff.

i. Anti-Money Laundering controls:

The responsible Anti Money Laundering Officer must ensure by adequate customer-and business related controls that all applicable AML requirements are being adhered to and security measures are properly functioning.

j. Anti-Money Laundering Training:

All employee (including trainees and temporary personnel) must undergo anti money laundering training.

k. Sanction Requirements:

NMB Group will adhere to all applicable sanction requirements and will check clients and transactions against applicable sanction lists.

l. Acts, Regulations, Policies and Procedures:

Each entity forming part of NMB Group shall have AML-CFT policies and procedures in place which shall be reviewed annually. The AML Officer of respective entity must ensure the

compliance of Group AML-CFT policy and respective entity's AML-CFT policy. Further NMB Bank Ltd., NMB Laghubitta Bittiya Sanstha Limited. must ensure adherence with regulations and guidelines issued by Nepal Rastra Bank whereas NMB Capital Ltd. and NMB Securities Ltd. as licensed and regulated by Securities Exchange Board of Nepal must ensure adherence with regulations and guidelines issued by Securities Exchange Board of Nepal (SEBON).

4. Roles and Responsibilities

The following is a description-of the roles and responsibilities of functions involved in the matters covered by this policy.

Group entities shall have an appropriate organizational and governance structure to identify, prevent and detect money laundering and terrorist financing, report in line with the requirements established in law, and block or freeze funds or economic resources following application of controls of sanctions or international financial countermeasures.

Group entities shall have at least one person responsible to oversee the implementation/application of this policy and enter into dialogue with local regulators (respective regulators) if necessary. Further, holding company (i.e. NMB Bank Ltd.) shall annually review the reports issued by auditors, regulatory bodies etc. of subsidiaries to ascertain the compliance with AML-CFT regulations by NMB Audit Team. Non-Compliance final findings in AML/CFT regime by audit shall be immediately shared with NMB Bank AML unit without fail.

Afore-mentioned roles and responsibilities must be exercised respecting the three lines of defense.

a. First line of defense

As a general rule and in the context of AML/CFT, the business and support units are the first line of defense in charge of identifying, assessing and controlling the risks of their business. They should know and carry out the policies and procedures and be allotted sufficient resources to do this effectively. As part of the first line of defense, policies and procedures should be clearly specified in writing, and communicated to all personnel. They should contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the bank in compliance with regulations. There should be internal procedures for detecting and reporting suspicious transactions.

b. Second line of defense

Risk and Compliance (including AML), as the second line of defense, will provide independent challenge and oversight of the risk management activities performed by the first line of defense This second line of defense should ensure that risks are managed in accordance with the risk appetite defined by senior management and promote a strong risk culture throughout the organization.

As an independent second line of defense, the Compliance/AML function is responsible for monitoring and overseeing risks arising from AML/CFT and sanction programs, assessing the impact on risk appetite and the risk profile of the entity and taking account of the provisions of this framework. They will develop and implement the necessary policies and procedures to property manage and control the prevention of money laundering and terrorist financing and sanction programs.

The Risk function shall be responsible for integrating and consolidating the risks arising from conduct and reputational risks, assessing the impact on risk appetite and the risk profile of the entity, and taking account of the provisions of this policy. They also add conclusions to specific risk information in such a way as to present a complete picture of the full range of risks to which the entity or the Group is exposed.

c. Third line of defense

As part of the third line of defense the Internal Audit Function regularly assesses that policies, methods and procedures are adequate and effectively implemented for the management and control of the system for the prevention of money laundering and terrorist financing for compliance with sanction programs in the Group, providing an independent assessment.

5. Record Retention

Records must be kept of all transaction data and data obtained for the purpose of identification as well as of all documents related to money laundering topics (e.g. files on suspicious activity reports, documentation of AML account monitoring, etc.). Those records must be kept for a minimum of 7 years. However, records of PEP customers must be retained for at least 10 years of giving up a particular function.

6. Ownership

This document must be approved by the Board of NMB Bank Limited. The Board of NMB Bank is responsible for the interpretation of this policy.

7. Validity Date and Periodic Review

This policy will be effective on a Group-wide basis from the date of approval by NMB Bank Ltd Board of Directors. Its contents will be reviewed periodically, and any changes or modifications will be made as appropriate.