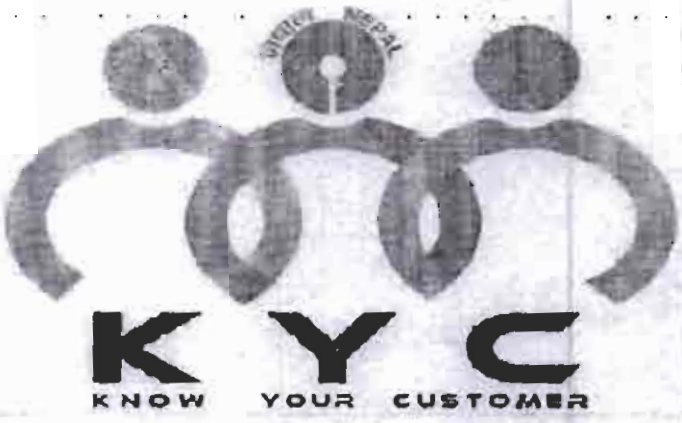
नेपाल एसबिआई बैंक लिमिटेड

NEPAL SBI BANK LTD.



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

Reviewed on 10th May 2024

Version Control

Version Number	8.00
Owner of Document	Compliance Department
Reviewed By	Internal Audit Department, Legal Department & Integrated Risk Management Department
Approved By	Board of the Bank
Effective date	Date of circulation.

The policy shall be reviewed as and when necessary or at least annual intervals.

Document History

Version Number	Approved by BOD		Revision Description
	Meeting no.	Date (MM/DD/YY)	
1.0	295	30.04.2011	
2.0	364	26.06.2014	
3.0	403	24.01.2017	
4.0	424	17.06.2018	
5.0	442	15.11.2019	
6.0	474	29.09.2021	Approved by Board of the Bank subject to incorporation of suggestions/ feedback of SBI, IBG.
	478	13.12.2021	Incorporation of the suggestions/ feedback of SBI, IBG.
7.0	499	12.04.2023	Segregation of Policy and Procedures of KYC, AML & CFT
8.0	513	10.05.2024	

Table of Contents

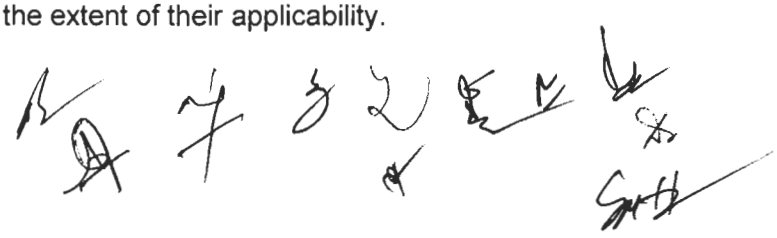
Preamble

Asset (Money) Laundering Prevention Act, 2064 (ALPA) and Asset (Money) Laundering Prevention Rules, 2073 (ALPR) formulated by Government of Nepal are in force in the country for the purpose of preventing the country from the risk of asset (money) laundering and terrorist financing. Moreover, Nepal Rastra Bank (NRB) has issued its directives in relation to prevention of asset (money) laundering and combating of financing of terrorist activities to be followed by Banks and Financial Intuitions (BFIs). Financial Intelligence Unit of Nepal (FIU-Nepal), the financial intelligence unit of the country, responsible for receiving, processing, analyzing and disseminating financial information and intelligence on money laundering and terrorist financing activities, also prescribes the guidelines and standards to be followed by BFIs.

Being a joint venture bank as well as foreign subsidiary of State Bank of India (SBI), Nepal SBI Bank Ltd. (NSBL) has also taken into cognizance AML/CFT Policy of State Bank of India (SBI) to the extent of applicability.

Therefore, with a view to address and comply with the provisions of ALPA, ALPR, Directives of Nepal Rastra Bank and guidelines of FIU-Nepal in respect of AML/CFT and to formulate necessary policy to combat Assets (Money) Laundering and Combating of Financing of Terrorism, the Bank's Board of Directors has reviewed this Know Your Customer (KYC), Anti Money Laundering (AML) and Combating of Financing of Terrorism (CFT) Policy of the Bank in line with the stipulations of ALPA, ALPR and Directives of Nepal Rastra Bank and FIU-Nepal.

KYC, AML & CFT Policy hence, encompasses, inter alia, provisions stipulated under recommendations of Financial Action Task Force (FATF), which serve as the international standard for combating money laundering and financing of terrorism and proliferation of weapons of mass destruction and relevant provisions prescribed by State Bank of India (SBI) through its AML/ CFT Guidelines for Operating Units to the extent of their applicability.



1. Objectives of the Policy

The Primary objective of this policy is to prevent the Bank from being used, intentionally or unintentionally for money laundering or terrorist financing activities. The Policy further enable the Bank to know/understand the customers and their financial dealings better and manage the risks prudently. Objectives proposed to be served by the Policy in relation to compliance of KYC, AML & CFT provisions are:

i) To lay down policy framework of the Bank for abiding by the KYC Norms, AML and CFT measures as set out by NRB, based on the provisions under ALPA, ALPR and FATF guidelines.

ii) To enable the Bank to verify the bona-fide identification of customers and beneficial owners and their financial dealings, which in turn would help the Bank to get information of transactions, monitor and manage risk prudently.

iii) To establish Customer Due Diligence measures as a guiding principle for Bank's business practices.

iv) To set up adequate arrangement for maintaining higher morale of employees, inter alia, during their selection and appointment.

v) To prescribe appropriate mechanism for training and development to officials and employees on AML/CFT laws, policies and procedures.

vi) To arrange for effective mechanism for independent monitoring, supervision, control, audit and updating records thereof.

vii) To arrange for adequate mechanism for identification and reporting of unusual and suspicious activities/transactions.

viii) To put in place required arrangement for accomplishing the responsibilities as per ALPA, rules framed thereunder, NRB Directives and assessing effectiveness of the same.

ix) To establish basis and system of risk assessment.

x) To establish system for risk-based customer identification, updating identification details and ongoing monitoring.

xi) To set up the system for dissemination of information related to terrorist individual, group or organization and confiscation of asset or fund of such terrorist individual, group or organization and reporting.

xii) To establish the system for maintenance of records as per the requirement of the prevailing Act, rules and norms.

xiii) To establish the mechanism for filing required reports including threshold transactions.

xiv) To specify internal roles and responsibilities and internal control mechanism.

xv) To comply with the provisions of the ALPA, rules framed thereunder and NRB Directives.

The focus of the KYC, AML & CFT Policy is on obtaining comprehensive information regarding new customers at the initial stage and that of existing customers over a predetermined period, thereby establishing the bona-fides of customers opening accounts and/or conducting transactions and identifying and keeping a watch on high value transactions and those of suspicious nature, as well as reporting them to Law Enforcement / Regulatory authorities, as and when required.

2. Scope and Applicability of the Policy

This policy is applicable to all branches/extension counters, province offices, departments, Corporate Office, banking subsidiaries of the Bank and is to be read in juxtaposition with related policies /procedural guidelines/circulars/office orders/instructions issued by the Bank from time to time.

The contents of the policy shall always be comprehended auto-corrected with the amendments/revisions/modifications which may be advised by NRB, FIU-Nepal and / or by ALPA/ALPR or by Bank through internal circulars from time to time.

3. Definitions and Explanations of Terms used in the Policy

Definitions and explanation of the terms used in this policy are as under:

i) Customer

"Customer" is defined as a person or entity that maintains or attempts to establish business relationship or conducts or intends to conduct any transaction with the bank. Following person or entity also falls under the ambit of customer.

- A person or an entity that maintains an account and/or has a business relationship with the Bank in any way (e.g. borrowers and guarantors of loan sanctioned by the bank, Demat account holders, Locker holders etc.)
- A person or an entity on whose behalf the account is maintained i.e. the beneficial owner.
- Beneficiaries of transactions conducted by professional intermediaries (e.g. Stock Brokers, Chartered Accountants, lawyers etc.), as permitted under the law.

- Any person or entity connected with a financial transaction with the Bank.

ii) Transaction

"Transaction" means purchase, sale, distribution, transfer, investment, use or any type of agreement or any of the following acts performed for any type of economic or business activities:

- Establishment of business relation.
- Opening of an account.
- Deposits or collection of funds, payment, payment order, exchange or transfer of fund in whatever currency, whether in cash or by cheque or other instruments through electronic or any other means.
- The use of a safe deposit (Locker).
- Establishing any fiduciary relationship.
- Any payment made or received in whole or in part based on any contractual or other legal obligation; or
- Establishing or creating a legal entity or legal arrangement.

iii) Beneficial Owner (BO)

"Beneficial Owners" or "Ultimate Beneficial Owners" refer to those natural persons, who are ultimate beneficiaries or owners of any legal person. Beneficial owners directly or indirectly, own, control, direct or influence customers/ transactions, assets, legal entity or legal arrangement. Beneficial owner of a natural person is the one on whose behalf account is operated or a transaction is being conducted. Beneficial owner enjoys the benefit of ownership even though the title of some form of property is in the name of another customer.

iv) Politically Exposed Person (PEP)

Politically Exposed Persons are individuals who are or have been entrusted with prominent public function in the country or abroad. However, the definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. Politically Exposed Person (PEP) includes Domestic PEPs, Foreign PEPs, and PEPs of International Organizations. It further denotes the person specified as PEP by Government of Nepal by publication through Nepal Gazette

at the recommendation of National Coordination Committee. PEP can be categorized as under:

- **Domestic PEP**

It includes following officials and any person having such responsibility or having been designated such responsibility:

- President
- Vice-president
- Prime Minister
- Chief justice
- Speaker and deputy speaker of House of Representatives
- Chairman and vice-chairman of National Assembly
- Governor of province
- Minister of Government of Nepal
- Chief minister of provincial government
- Member of federal parliament
- Officials of constitutional bodies
- Speaker & deputy speaker of provincial assembly
- Ministers of provincial government
- Officials of Government of Nepal at special class and secretary level or its equivalent or higher position
- Judge of high court or that of higher level
- Members of provincial assembly
- Central level officials of national level political parties
- Head and deputy head of district coordination committee
- Mayor and deputy mayor of municipalities
- Chairman and vice-chairman of rural municipalities
- Senior officials of the institutions owned fully or partly by government.

- **Foreign PEP**

It includes foreign head of the state, head of the government, senior politician, central level officials of national level political parties, top level administrator, senior judicial authorities, senior security officials, senior officials of state-

controlled institutions or the person having such responsibility or having been designated such responsibility.

- **PEP of International Organization**

  It includes board member, manager, director, deputy director having been assigned top level responsibility of international organization or the person having similar responsibility or having been designated such responsibility.

v) **Correspondent Banking**

Correspondent banking is the facility of banking services provided by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through accounts, cheques clearing etc.

Section 2(g) of ALPA has defined correspondent Banking as an arrangement of providing banking service to its customer by a financial institution through other financial institution.

vi) **Downstream Correspondent (Nested) relationship**

A downstream correspondent (also referred to as "nested") relationship occurs when a Correspondent Bank client provides correspondent services to other banks, domiciled Inside or outside their country, to facilitate international products and services on behalf of the Downstream Correspondent's clients. This is a practice where a respondent bank provides downstream correspondent banking services to other financial institutions and processes these transactions through its own correspondent account.

vii) **Payable-through Accounts (PTA)**

Payable-through accounts, also terms as "Pass-through account" or "Pass-by accounts", are the correspondent accounts that are used directly by third parties to transact business on their own behalf. In other words, the institution providing the correspondent banking services allows its correspondent Banking Clients' accounts to be accessed directly by the customers of that correspondent, e.g., the customers of the correspondent may have cheque writing privileges or otherwise

be able to provide transaction instructions directly to the institution or through a sub-account.

viii) **Shell Entity**

Shell Entity means a firm/company that is incorporated for legitimate business purposes but has no independent assets or operations of its own. It serves as a vehicle for business transactions and may be used by its owners to conduct specific business dealings or maintain control of other firm/companies. Shell entities may not be illegal as they may have legitimate business purposes. However, they can also be a main component of underground activities, especially those based in tax haven countries.

ix) **Shell Bank**

Shell Bank refers to Financial Institution or group of financial institutions that has no physical existence in the country of incorporation or license or Financial Institution or group of financial institutions that is not under any regime of effective regulation and supervision.

x) **Offshore Entity**

The term *offshore entity* has two definitions depending on its perspective. From the standpoint of the principals of the company, it is a company that has been filed outside of the country where its principals (officers, directors, shareholders, members, partners etc.) reside. From within its country of formation, it is a company that has been formed for the purpose of operating outside of the jurisdiction where it was originally filed.

xi) **Offshore Bank**

An offshore bank is a bank located in a jurisdiction different from that where its depositors reside. Offshore banks usually prohibit the bank from establishing business activities in the jurisdictions of establishment. An account held in a foreign offshore bank is often described as an offshore account.

xii) **Non-face-to-face customers/ transaction**

Non face-to-face customers are those with whom the Bank branch has not had direct face to face interaction at the time of establishing business relation i.e.

customers who open the account without visiting the Branch. Similarly, non-face-to-face transaction is where a transaction occurs without a customer having to be physically present i.e. mobile banking, internet banking, debit/credit cards etc.

xiii) Walk-in-Customers

The customers who intend to conduct a transaction or establish any type of business relation with the Bank without having his/her/own account with the Bank.

xiv) Walking Accounts

A Walking Account is an account for which the account holder has provided standing instructions that upon receipt all funds should be immediately transferred into one or more accounts. By setting up a series of walking accounts, criminals can automatically create several layers as soon as any fund transfer occurred.

xv) Escrow Accounts

Escrow Account is an account which is opened by a third party on behalf of two other parties that are in the process of completing a general transaction such as purchase/sale of goods or properties. In case of such accounts, the funds of a party are held by the escrow agent in escrow account for payment to the other party upon receipt of appropriate instructions from them or until predetermined contractual obligations have been fulfilled.

For example, a company selling goods wants to be certain that it will get paid when the goods reach their destination. Conversely, the buyer wants to pay for the goods only if they arrive in good condition. The buyer can place the funds in escrow account and give irrevocable instructions to disburse them to the seller once the goods arrive. This way, both parties are safe, and the transaction can proceed.

xvi) Customer Due Diligence (CDD)

Customer Due Diligence is a process by which the Bank collects, independently verifies and analyzes the information about a customer that enables the Bank to assess the extent to which the customer exposes it to a range of risks especially the risk of money laundering and terrorist financing. If CDD leads to a high-risk determination, the Bank is required to conduct an Enhanced Customer Due Diligence.

xvii) Simplified Customer Due Diligence (SCDD)

Simplified Customer Due Diligence (SCDD) is the lowest level of due diligence that can be applied to a customer. This is appropriate for the customers who has lowest risk of involving in money laundering and terrorist financing through Bank's services or customer becoming involved in money laundering or terrorist financing.

xviii) Enhanced Customer Due Diligence (ECDD)

Enhanced Customer Due Diligence (ECDD) refers to additional due diligence pertaining to the identity of the customer, source of income, nature and value of transaction etc. for the customer posing high risk. Enhanced Customer Due Diligence (ECDD) is required where the customer and product/service combination are considered to be a higher risk.

4. Know Your Customer (KYC), Money Laundering and Financing of Terrorism

4.1 Know Your Customer (KYC)

"Know Your Customer (KYC)" is a process of identifying the customer, verifying their identity, monitoring their transactions and reviewing their profiles on risk-based approach and adopting necessary measures to protect the Bank from being the vehicle of money laundering. It is the documented norms for the Bank which enables it to acquire the information pertaining to its customers/clients and the legitimacy of its business/transactions so as to prevent potential risks. It requires due diligence that the Bank must implement to identify its clients and obtain relevant information as detailed as possible pertaining to the dealings or doing business or financial transactions with them. It is the measures implemented to validate the legitimacy of the customers' transactions and their information.

In this regard, it is absolutely imperative to know clearly the customer identity, source of fund/assets and nature of transaction. Proper documentation for the KYC should be a pre-condition.

4.2 Money laundering

It is a process by which criminal disguises the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source. It is the process whereby proceeds of crimes such as drug trafficking, smuggling (alcohol, arms), kidnapping, gambling, robbery, counterfeiting, bogus invoicing, tax evasion, misappropriation of public funds and

the like are converted into legitimate money through a series of financial transactions making it impossible to trace back the origin of funds. Most often, such clandestine deals are the first step in using the banking system to launder or clean up the cash obtained from trade of illegal goods or services. Once the money is placed within the Bank, it goes through an intricate web of transactions, better known as layering, that leave no audit trail. Conversion of this unofficial or black money into official currency thereby 'changing its colour' is money laundering.
In this regard, Anti Money Laundering (AML) refers to a set of procedures, laws and regulations designed to stop the practice of Money Laundering.

Under Section 3 of Chapter 2 of ALPA "Offences of money laundering" has been defined as under:

Assets are supposed to have been laundered if anyone commits any of the following acts:

i) Converting or transferring property by any means knowingly or having reasonable grounds to believe that it is proceeds of crime for the purpose of concealing or disguising the illicit origin of property, or assisting any person involved in the offence for evading legal consequences of offender.
ii) Concealing or disguising or changing the true nature, source, location, disposition, movement or ownership of property or rights with respect to such property knowingly or having reasonable grounds to believe that it is proceeds of crimes.
iii) Acquiring, using, possessing any asset knowingly or having reasonable grounds to believe that it is the proceeds of crime.

No person shall conspire, aid, abet, facilitate, counsel, attempt, associate with or participate in the commission of the acts mentioned above.

Money launderers use the banking system for cleansing 'dirty money' obtained from criminal activities with the objective of hiding/disguising its source. The process of money laundering involves creating a web of financial transactions so as to hide the origin and true nature of these funds.

4.3 Financing of Terrorism

Financing of terrorism refers to the activities that provide financing or financial support to individual terrorists or terrorist groups or terrorist organizations.

Under Section-4, Chapter 2 of ALPA, provisions in regard to combating of financing of terrorism has been stipulated under the point "Terrorist Activities not to be financed" as under:

i) No person shall, by any means, directly or indirectly, with unlawful intention and willfully, provide or collect funds or assets, in spite of having knowledge that such funds or assets shall be used or may be used, in whole or in part, in order to carry out a terrorist act or by a terrorist or a terrorist organization.

ii) No person shall attempt for carrying out any act as mentioned above.

iii) No person shall provide or conspire to provide material support or resources to any terrorist or terrorist organization by any means, directly or indirectly, in order to carry out a terrorist act.

iv) In relation to any of the acts mentioned above, no person shall commit any of the following acts:
   a) To participate as an accomplice in such act,
   b) To organize or direct others to commit such act,
   c) To contribute a group of persons which commits such act or has a common purpose of committing such act or willfully promote such group of persons for furthering their criminal activities or to achieve such purpose.

v) Even if any of the following circumstances exist in relation to any act mentioned above, It shall be the offence of terrorist financing:
   a) Terrorist act does not occur or is not attempted,
   b) Assets or funds are not actually used to commit terrorist act or attempt thereof.
   c) Assets or funds are linked or not linked to a specific terrorist act.
   d) Terrorist act or intended terrorist act occurs or will occur in the country, state or territory where such act was intended to occur or somewhere else,
   e) Individual terrorist or terrorist organization is located or not in country, state or territory where the person committing such act resides or somewhere else.
   f) Whether the assets or funds are collected or made available from legitimate or illegitimate, any source or means.

If any person commits any of the activities as mentioned above, the same shall be offense of financing terrorist activity.

Even if any act or offence mentioned above is committed in the foreign country or territory provided that the act is treated as offence under the law of respective country, the same shall be treated as the offense of Money laundering and Terrorist financing committed in Nepal.

For the purpose of this document, the term money laundering/ terrorist financing would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of the funds.

4.4 Money Laundering Process

There are three stages involved in money laundering: placement, layering and integration.

i) Placement

It is the initial stage of money laundering, where "dirty" cash or proceeds of crime from the source enters into the financial system. Generally, this stage serves two purposes:

a) It relieves the criminal from holding and guarding large amounts of bulky cash; and
b) It places the money into the legitimate financial system.

It is during the placement stage that money launderers are the most vulnerable to being caught. This is because placing large amounts of money (cash) into the legitimate financial system may raise suspicions of officials.

ii) Layering

The second stage in money laundering is layering. In this stage, money launderers carry out series of conversions or movement of fund mostly to distance from their original source. By way of layering, launderers make it more difficult to detect and uncover a laundering activity. It is meant to make the trailing of illegal proceeds difficult for the law enforcement agencies.

iii) Integration

The final stage of the money laundering process is termed as integration. It is at the integration stage where the money is returned to the criminal, after series of transactions, from what seem to be legitimate sources. Having been placed initially as cash and layered through a number of financial transactions, the criminal proceeds are now fully integrated into the financial system and can be used for any purpose.

4.5 Money Laundering Area

Three stages of money laundering placement, layering and integration always do not take place simultaneously rather they may occur separately or overlap. Though money laundering can practically take place anywhere in the world, money launderers tend to seek out areas in which there is a low risk of detection due to weak or ineffective anti-money laundering programs.

Money laundering activities may be concentrated more at a place or territory based on the stage of money laundering at which the funds have reached. For example, the funds are usually processed in the proximities of the underlying criminal activity especially in the country where it originated, though always it may not be the case. In the stage of layering, the launderer might choose an offshore financial center, a large regional business center, or a world banking center – any location that provides an adequate financial or business infrastructure.

Finally, at the integration phase, launderers might choose to invest laundered funds in still other locations if they were generated in unstable economies or locations offering limited investment opportunities.

Among others, a latest trend in money laundering involves use of the new technologies, like smart Cards, online Banking, electronic Cash, trade transactions, cryptocurrencies, etc. To prevent the bank from being used as a vehicle of money laundering through new technologies, the bank requires being vigilant and should administer the robust controlling, monitoring and reporting system.

5. Policy Framework

The bank shall follow the applicable international as well as domestic legal framework in relation to AML/CFT.

5.1 International Framework

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global anti-money laundering (AML) and combating of financing of terrorism (CFT) standard. FATF's Forty Recommendations revised and adopted in 2012 set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot take all identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. Recommendations of FATF and other functional bodies like Asia/Pacific Group on Money Laundering (APG), International Monetary Fund (IMF) and World Bank shall be taken into cognizance by the Bank as applicable.

Further, the standards prescribed by United Nations and Basel Committee for Banking Supervision (BCBS) shall also serve as the basis for the Bank for combating money laundering and terrorist financing where mandatory/applicable.

5.2 Domestic Framework

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

i) Asset (Money) Laundering Prevention Act, 2064 (Including amendments) (ALPA)

ii) Asset (Money) Laundering Prevention Rules, 2073 (ALPR)

iii) Asset (Money) Laundering Prevention (Freezing Asset or Fund of listed individual, group or organization) Rules, 2070

iv) Unified Directives No. 19 on AML/CFT issued by Nepal Rastra Bank and its respective amendments.

v) Directives/Guidelines issued by FIU-Nepal (AML/CFT Directives to Financial Institutions)

   a. Directives to implement UNSCR (United Nations Security Council Resolutions) 1267 & 1373

b. Threshold Transaction Reporting Guidelines
c. Suspicious Transaction Reporting Guidelines

5.2.1 Obligations of Bank under ALPA

Section 7(P) and 7(R) of ALPA has stipulated following obligations of the Bank, in addition to others:

i) The Bank shall develop and implement AML/CFT Policy and Procedures compatible with its nation, territory, working area, size of business, customer, transaction and risk of money laundering and financing of terrorism for the compliance of the provisions stipulated under ALPA, ALPR and directives thereunder. The policy and procedures so developed should include following components:

a. Internal policies, procedures and control arrangement relating to customer identification, business relation, monitoring, transaction information/reporting, record keeping and other obligations.

b. Arrangement for ongoing monitoring.

c. Arrangement to implement obligations as per ALPA, its rules and directives thereunder.

d. Adequate procedural arrangement for ensuring high standard of employees, inter alia, during selection and appointment.

e. Arrangement for ongoing training and development to employees,

f. Effective arrangement for independent monitoring, review and audit of the activities and updating the records.

g. Measures for detection and reporting of suspicious transaction,

h. Other measures required for fulfilling the obligations as per ALPA, ALPR and NRB Directives and other arrangement required for evaluation of effectiveness of the same.

i. Other measures as prescribed by the Regulator.

ii) Bank shall have to appoint compliance officer of managerial level to comply the obligation pursuant to the provision of ALPA, its rules and directives thereunder. The Bank shall have to ensure following function, rights and duties of the compliance officer and required resources for the same:

a. Have access to any of the required records, books of accounts and related documents in the course of delivering his/her responsibility.

b. Seek for and obtain data, information, details or documents from concerned employee of the Bank.

c. Perform other necessary functions for implementation of ALPA, its rules and directives thereunder.

d. Perform other functions as prescribed by the regulator

iii) The Bank shall maintain records, as under, accurately and securely for minimum five years after the termination of business relationship or from the date of transaction or from the date of occasional transaction:

a. All documents and records related to identification and verification of customer and beneficial owner,

b. All documents, records and conclusion of the analysis of customer or beneficial owner and transaction,

c. All documents regarding report of suspicious transaction for the period of five years.

d. All documents, details and records related to accounting and business relation of the Bank

e. All documents, details and records relating to domestic and foreign transactions,

f. All documents, details and records of attempted transactions,

g. All other documents, details and records as prescribed by regulators.

iv) The Bank shall maintain documents, details and records as mentioned above in such a way that each of the transactions is clearly visible and sufficient to be produced in the course of legal action as evidence.

v) The documents, details and records shall have to be maintained in such a way that the same could be made readily available to competent authorities upon demand.

vi) Other arrangement in regard to preservation and maintenance of documents, detail and records shall be as prescribed.

As per the provision stipulated under Section 7(V) of ALPA, regulator may impose stipulated action/actions and punishment if the Bank does not comply with the order, direction or prescribed standard issued as per ALPA, rule or directives issued thereunder.

5.2.2 Obligations of FIU under ALPA

Section 9 and 10 of ALPA have stipulated following major duties, functions and rights of FIU in relation to the reporting entities including banks:

i) Receiving reports on threshold transactions, suspicious transaction and any other information, details and documents related to money laundering and terrorist financing from financial institutions and non-financial institutions as per ALPA.

ii) Carrying out analysis of suspicious transaction report and any other report and information received as per the provisions of ALPA and forwarding the conclusion of analysis to Department of Money Laundering Investigation or any other agencies engaged in the investigation as per the prevailing laws if found suspicious of the offense of money laundering or financing of terrorism or any other offense.

iii) Arranging for trainings to its employees, reporting entities, related agencies and regulating bodies as per requirement.

iv) Providing necessary feedback or guidelines to reporting entities or concerned agencies in regard to detection of suspicious transaction and report and information of suspicious transactions.

v) Assisting regulating bodies for inspection of reporting entities in regard to detection, evaluation and reporting system of suspicious transactions and their effectiveness or providing feedback based on the report of inspection and supervision.

vi) Developing understanding with foreign agencies, performing similar function, for mutual cooperation.

vii) Seeking required information or assistance from FIUs or agencies performing similar function in the foreign countries and providing required information or support to them at their request.

viii) Seeking for and obtaining required additional document, record, details and information from reporting entities where required.

ix) Issuing direction to reporting entities in regard to reporting requirements where required

x) Imposing penalties, up to the amount of Rs. 10,00,000.00 (Rs Ten Lacs), to reporting entities based on the severity of non-compliance if they do not comply with the reporting requirements in regard to suspicious transactions or if they do not abide by the order/instruction issued or do not produce the information/documents demanded.

6. KYC/ AML/ CFT Risk Management / Perception

Non-compliance with KYC/AML/CFT standards can lead to use of banking products and services including the technology channels of the Bank for Money Laundering/terrorist financing activities and thus expose the Bank to risks such as Operational Risk, Reputation Risk, Compliance Risk, Legal Risk etc.

Failure to comply with the Anti-Money Laundering regulations constitutes an offence and those not complying with the law will find their reputation severely damaged and details of the offence published in the local/national/international press. Bank should therefore comply with the prevailing laws and regulations in order to protect good name and reputation of the Bank, decrease the likelihood of becoming a victim of fraud or illegal activity, and ensure safe and sound business practices for customers.

6.1 Roles & responsibilities

As mentioned earlier, the compliance function is the roles and responsibilities of each and every staff in the organization. Roles and responsibilities of various authorities in regard to AML/CFT compliance in the Bank shall be as under:

6.1.1 Board of Directors (BOD)

Board of the Directors of the Bank shall formulate internal policy and procedure for compliance of AML/CFT provisions as per ALPA, ALPR, NRB Directives and international standards of AML/CFT applicable to the Bank. The Board shall carry out the review of the report submitted by Assets (Money) Laundering Prevention Committee of the Board (ALPC) and activities carried out thereon. It shall maintain oversight over management of money laundering risk and terrorist financing risk through reports so received from ALPC or other committees of the Board constituted as per the provisions of NRB Directives. It shall review KYC, AML & CFT Policy at least once in a year. However, the policy may further be reviewed by the Board of Director any time before one year based on need basis.

6.1.2 Assets (Money) Laundering Prevention Committee of the Board (ALPC)

Assets (Money) Laundering Prevention Committee of the Board (ALPC) constituted as per the provisions of NRB Directives shall oversee the implementation of AML/CFT Policy and procedure of the Bank along with compliance of AML/CFT provisions as per ALPA, ALPR and NRB Directives. ALPC shall comprise the following members:

Non-Executive Director	- Coordinator
Chief Operating Officer (COO)	- Member
Head Compliance Vertical / CRCO	- Member
Head – Integrated Risk Management Department	- Member
Compliance Officer appointed as per point No 18(2) of NRB Unified Directives No 19	- Member Secretary

ALPC shall meet at least once in three months unless otherwise required with the presence of at least three members including Coordinator and Member Secretary.

ALPC discuss about the AML/ CFT related issues of the Bank and submit the report of the activities undertaken for prevention of Money Laundering and Terrorism Financing to Board of the Bank at least once in every three months. Duties and responsibilities of the ALPC shall be:

- To review activities performed as per Assets (Money) Laundering Prevention Act, Assets (Money) Laundering Prevention Rules and NRB Directives No. 19 and submit the report to Board of Directors.
- To discuss the adequacy of internal policy, procedure and procedural aspects formulated and implemented in accordance with the Money Laundering Prevention Act 2064, Money Laundering Prevention Regulations 2073, NRB Directives and recommendations issued by FATF and to make necessary policy arrangements and implement them.
- To discuss on process adopted and to be adopted for identification and prevention of money laundering and terrorist financing activities adequacy of IT system adopted for the same and put-up the suggestions to Board of the Bank for necessary improvement.
- To analyze arrangement regarding customer identification, formulate and implement/ get implemented the customer identification and customer Acceptance Policy based on risk category, PEP and beneficial owner in an effective way.
- To submit quarterly report to Board of the Bank on status of compliance and implementation of Assets (Money) Laundering Prevention Act, Assets (Money) Laundering Prevention Rules, NRB Directives and Bank's internal policy.
- To receive following details/ reports from Management, discuss on the same and provide necessary suggestion to Board of Directors as per the requirement
  i) Report regarding AML/CFT Risk Management
  ii) Updated status of customer identification, details of CDD/ PEP/ ECDD & details regarding policy/procedure/institutional reforms to be implemented in future for its prompt, easy and enhanced efficiency with the use of Information Technology.

iii) Review of AML/ CFT related observations of internal audit report/external audit report/ NRB inspection report to be made and necessary policy and procedural reforms to be made in this regard.

- To analyze ML/TF risk associated with launch of new service/facility, purchase of IT system, wire transfer, transfer of fund through e-banking/ mobile banking (including QR Code), mobile wallet, online/ offline transaction and discuss for necessary reforms required in policy & procedural aspects for managing such risk.
- To analyze national and international issues/ incidents related to ML/TF and impacts that may fall on Bank and Financial Institutions and provide suggestion to Board of the Bank in regard to necessary policy arrangement for management of such risk.
- To manage necessary and suitable knowledge transfer programme on AML/CFT for compliance officer, shareholders holding 2% or more shares of paid-up capital, board members, top management and employees directly and continuously involved in AML/CFT function.
- To review adequacy of internal policy arrangement and guidelines on AML/CFT on regular basis and provided suggestion to Board of the Bank.
- To ascertain whether AML/CFT system has functioned effectively or not, whether risk has been managed suitably or not, whether unusual activity has been monitored adequately or not and whether necessary reporting has been made to concerned authorities or not and arrange for discussion on such matters in the meeting of Board of Directors.
- To discuss whether details/ reports related to AML/CFT to be submitted to FIU and to concerned authorities as specified through the mode prescribed by Nepal Rastra Bank has been submitted or not without violating the provision of 44a of Assets (Money) Laundering Prevention Act 2064.
- Programme for Anti Money Laundering and Combating of Financing of Terrorism should be formulated on the basis of risk by Board of the Bank. ALPC to develop mechanism for ensuring effective implementation of such programme/ budget and regular monitoring.

6.1.3 Operational Risk Management Committee (ORMC)

Operational Risk Management Committee (ORMC) reviews operational risk related matter to mitigate the operational risk in Bank. AML/CFT related issues are also deliberated in the ORMC. It analyzes the gap if any with regard to compliance to AML/CFT provisions and provides suggestion, feedback and instruction for the compliance of the same.

In addition, there exists a Central Management Committee in the Bank (CENMAC) comprising high level management officials. The committee may, review, based on need, the status of implementation of AML/CFT guidelines in the Bank and provide necessary instruction, suggestion and action plan to the concerned departments/offices/branches for ensuring implementation of AML/CFT guidelines.

6.1.4 Chief Risk and Compliance Officer (CRCO)

Chief Risk and Compliance Officer, a senior management level official, is entrusted with oversight responsibility of managing ML/TF risk in the Bank. CRCO shall provide necessary suggestion, feedback and extend required support to compliance department for ensuring effective compliance. He/ She shall have direct reporting line to RMCB and dotted line reporting to Managing Director & Chief Executive Officer of the Bank. He/she shall put up the report on activities undertaken by the Bank for compliance to AML/CFT measures and status of AML/CFT compliance of the Bank as per the provisions of ALPA, ALPR and NRB Directives to Assets (Money) Laundering Prevention Committee of the Board (ALPC) at least once in 3 months for review and further reporting by ALPC to the Board of the Bank. Such report, in addition to others, shall also include relevant information in relation to suspicious transaction report. He/she shall assist the Board and ALPC of the Board for managing the Bank's AML/CFT risks and formulating necessary policy/procedure/guidelines.

6.1.5 AML Compliance Officer

AML Compliance Officer deputed as per ALPA shall act as focal person to comply with the obligations pursuant to the provision of ALPA, ALPR and NRB directives and Bank's KYC/AML/CFT policy. The officer shall directly report to Chief Risk and Compliance Officer. Head of the Compliance

Department, who shall be at least managerial level official, shall be the AML Compliance Officer of the bank and the Member Secretary of Assets (Money) Laundering Prevention Committee of the Board (ALPC). The Bank shall report name, address, qualification, contact number, email address etc of the AML compliance officer to FIU-Nepal and report all such details of new incumbent in case of change. The Bank shall ensure following functions, rights and duties of the AML compliance officer and required resources for the same:

- Drafting policies, procedures and guideline for effective compliance of AML/CFT provisions as per ALPA, ALPR and NRB Directives.
- Analyzing and investigating the information related to suspicious and unusual activities received from departments, officials and employees.
- Seeking for and obtaining the service of experts from any department/officials and/or necessary data, information, details or documents from concerned employee of the Bank.
- Monitoring the compliance of the AML/CFT provisions as stipulated under ALPA, ALPR and NRB Directives and submitting the report to the ALPC/ Board of the Bank in a timely, complete, understandable and accurate manner so that it is equipped to make informed decisions.
- Recommending for departmental punitive action to the officials or employees who do not submit data, information, details, records or documents sought in the course of fulfilling the obligations as per the AML/CFT provisions of ALPA, ALPR and NRB Directives.
- Conduct the meeting of Assets (Money) Laundering Prevention Committee of the Board at least once in three months.
- Performing other necessary functions for implementation of ALPA, ALPR and NRB Directives.
- Performing other functions as prescribed by the regulator.

In addition to above functions prescribed by regulator, AML Compliance Officer shall have the following duties:

- Overall monitoring of implementation of Bank's KYC/AML/CFT policy.

- Monitoring and reporting of transactions, and sharing of information, as required under the law.
- Interaction with MLROs in Branches/Offices/Departments for ensuring full compliance with the Policy.
- Timely submission of Threshold Transaction Reports (TTRs) and Suspicious Transaction Reports (STRs) to FIU.
- Maintaining liaison with the law enforcement agencies, banks and other institutions which are involved in the fight against money laundering and combating financing of terrorism.
- Ensuring submission of periodical reports related to AML/CFT to the Top Management /Board level committees/Board.
- Updating the list of predicate offenses under the laws and circulating to the Branches/Extension Counters.
- Performing other KYC/AML/CFT compliance related functions as prescribed by FIU-NRB from time to time.

AML Compliance Officer shall be supported by necessary number of officers and staff posted at Compliance Department. In the course of discharging duties by AML Compliance Officer, he/ she shall regularly consult Chief Risk and Compliance Officer in regard to AML/CFT related issues, its compliance status and initiatives to be taken for improving the same. He/she shall be responsible for furnishing necessary information, documents, reports related to AML/CFT to NRB, FIU and investigating authorities, competent to receive such information/ documents as per the law as sought by them and confirming execution of order received from the competent authorities. While making any such correspondence/ communication, it shall have to be ensured that information in regard to investigation/inquiries about any customer or any other party is not tipped off by the concerned.

6.1.6 Assistant AML Compliance Officer & compliance functionaries

The officers posted at Compliance Department to support AML Compliance Officer are Assistant AML Compliance Officers. Assistant AML Compliance Officers at KYC/AML unit under Compliance Department shall have the responsibility of ensuring KYC/AML/CFT policy of the Bank along with the

AML/CFT provisions of ALPA, ALPR and NRB Directives. Assistant AML Compliance Officers and compliance functionaries at KYC/AML unit shall regularly monitor the transactions/ customer activities and communicate to the concerned employees, province offices, departments/ branches/ extension counters in regard to unusual transactions/suspicious activities and shall advise concerned employees/ branches/ offices/ departments for submission of related documents/information where required. While making any such correspondence/ communication, they shall ensure, on their part as well as on the part of the concerned, that there is no tipping off.

They shall monitor the compliance status of AML/CFT provisions, obtain information/report from the branches/extension counters, analyze the same and report to AML Compliance Officer. They shall regularly consult AML Compliance Officer in regard to AML/CFT matters and perform all other AML/CFT/Compliance related functions as assigned by AML Compliance Officer and/or deemed necessary.

Assistant Compliance Officers and compliance functionaries at Regulatory and Internal Compliance unit under Compliance Department shall also perform those functions where assigned by Compliance Officer and/or deemed necessary.

6.1.7 Department Head

Department Head is the ultimate authority at the respective department to ensure that AML/CFT provisions as per prevailing rules and regulations and bank's internal policy and procedures are complied with at the concerned department. He/she shall ensure that the AML/CFT guidelines are complied with while discharging the function of respective departments including establishing business relation, outsourcing services from third party and introducing any new product/service and reviewing existing product or service. He/she shall ensure that the business relation with the vendor/third party and their transaction are being regularly monitored to identify and report any unusual/ suspicious transactions. He/she shall further ensure that inquiry/ investigation about any customer and reporting of unusual / suspicious activity/ transaction are not tipped off by the concerned employees to any customer, unrelated staff or any other party as the same is punishable act.

6.1.8 Head-Province Office

Head-Province Office has the dual role of complying with the AML/CFT measures at the level of province office and monitoring the AML/CFT compliance status of the branches under his/her province. He/she shall ensure that the AML/CFT guidelines are complied with while discharging the function of the province office including establishing business relation, outsourcing services from third party etc. He/she shall have to ensure prompt reporting of prima facie suspicious transactions at the province office to the AML Compliance Officer.

During branch visit, he/she shall verify compliance status of AML/CFT measures of the branches falling under purview of province office and suggest appropriate actions to the branches/ extension counters for improving compliance culture in AML/CFT area. He/she shall coordinate with AML Compliance Officer and/or Human Resources Department for conducting trainings on KYC/AML/CFT matters where required. He/she shall further ensure that inquiry/ investigation about any customer and reporting of unusual / suspicious activity/ transaction are not tipped off by the concerned employees to any customer, unrelated staff or any other party as the same is punishable act.

6.1.9 Branch Manager/ Officer-in-charge of Extension Counters

Branch Manager/ Officer-in-charge of extension counter has the responsibility to ensure that AML/CFT provisions as per prevailing rules and regulations and bank's internal policy and procedures are complied with at the concerned branch/ extension counter. He/ she shall scrutinize the account opening request of the customer and ensure that the relevant KYC information/documents are obtained from the customers so as to identify and verify the customer and beneficial owners, proper due diligence has been carried out, sanction screening has been conducted, necessary approval for opening account has been obtained from higher authority where required and all other AML/CFT guidelines have been complied with before establishing business relation.

He/she shall ensure that the transactions of the customers are being monitored and all unusual/ suspicious transaction/ activity have been reported. He/she shall further analyze the observations of self-audit, internal/ external audit, regulatory inspection and all other inspection/ reports pertaining to AML/CFT measures of the branch/ extension counters and adopt appropriate corrective actions so as to ensure the rectification of such discrepancies and avoid recurrence of the similar issues. In case of transfer of staff or change in role and responsibilities of MLRO, he/she shall designate MLRO and reliever of MLRO immediately and report the same to Compliance Department. In Branch Manager's Monthly certificate (BMMC), he/she shall have to certify regarding compliance with KYC/AML/CFT guidelines and reporting of unusual /suspicious activity/transactions. He/she shall further ensure that inquiry/ investigation about any customer and reporting of unusual / suspicious activity/ transaction are not tipped off by the concerned employees to any customer, unrelated staff or any other party as the same is punishable act.

6.1.10 KYC Compliance Officer/Money Laundering Reporting Officer (MLRO)

Though AML Compliance Officer will have overall responsibility for maintaining oversight and coordinating with various functionaries in the implementation of KYC/AML/CFT policy and procedures, primary responsibility of ensuring implementation of KYC/AML/CFT Policy and related guidelines will be vested with the respective Branches/Offices/Departments.

For the purpose, each Department/Province Office/ Branch/Extension Counter will designate an official as KYC Compliance Officer/Money Laundering Reporting Officer (MLRO) who would ensure compliance of AML/CFT policy along with the AML/CFT provisions as per ALPA, ALPR and NRB Directives in their respective department/office/branch/extension counter. MLRO shall be the focal person for the respective department/office/branch/ extension counter and shall have the responsibility of ensuring compliance to AML/CFT provisions while establishing any business relation such as opening account, locker, conducting financial transaction, acquiring third party product/services, outsourcing, introducing new products/procedures as well as reviewing of existing

products/procedures and monitoring of the activities/transactions at their Department/Office/branch/extension counter from AML/CFT perspective. They shall adopt necessary measures to update customer identification status of existing customers including their beneficial owners as per the provisions of NRB Directives and Bank's KYC policy at least at the required frequency and as and when the need be. They shall monitor customer activities/ transactions on ongoing basis, carry out customer due diligence and enhanced due diligence as required. They shall further carry out investigation/ analysis in relation to any prima facie suspicious activity detected by them and reported by other staff members at their branch/ office so as to report the same to AML Compliance officer through Department Head/ Province Head / Branch Manager. They shall ensure that no business relation shall be maintained with banned individual/entity or/and with those falling in the sanction list. They shall further maintain confidentiality in relation to all activities/ transactions as per the extant guidelines and ensure that there is no tipping off in relation to any inquiries, investigation, reporting of unusual/ suspicious activity.

They shall report any unusual or suspicious activity/transaction to AML Compliance Officer through Department Head/Head of the office/Branch Manager/In-Charge of Extension Counter as applicable. To assist MLRO and to perform the functions of MLRO during his/her absence, the department/ office/branch/extension counter shall designate reliever of MLRO.

6.1.11 All Employees of the Bank

It is the responsibility of each and every staff of the Bank to understand the AML/CFT provisions applicable to their area of operation and ensure compliance of the same invariably. In this regard, all the employees of the Bank shall:

- Have through understanding of KYC, AML & CFT Policy of the Bank along with the provisions of ALPA, ALPR and NRB Directives.
- Comply with KYC/AML/CFT policy and procedures.
- Remain alert at all the times to the possibility of money laundering and reporting suspicious or unusual transactions to the concerned KYC

Compliance Officer/MLRO for further reporting to AML Compliance Officer.

- Make effective use of training and seek clarifications whenever necessary.
- Ensure that there is no tipping off.

Be aware that violation of ALPA, its rules and NRB Directive in relation to AML/CFT shall attract penalties including fines to the responsible staffs 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.

6.2 Control Function

6.2.1 Self Audit

As a part of risk focused internal audit, each branch/extension counter performs self-audit on half-yearly basis. During the self-audit, proper assessment and analysis in regard to implementation of AML/CFT measures, in addition to others, shall be conducted by the branches/ extension counters and appropriate actions shall be taken by them so as to improve compliance culture and avoid recurrence of discrepancies.

6.2.2 Control by Head-Province Office

Head-Province Office shall monitor AML/CFT compliance status of the branches/ extension counters falling under province office. He/ she shall further suggest branches/ extension counters in regard to appropriate actions to be undertaken for effective compliance and monitor the progress in this regard.

6.2.3 Internal Audit

Bank's Internal Audit will provide an independent evaluation of compliance with AML/CFT Policy including legal and regulatory requirements in regard to AML/CFT during their audit. During audit of branches/ extension counters, Internal Auditor shall check/ scrutinize AML/CFT compliance status at the branches at least once in eighteen months or at more frequent intervals during Risk Focused Internal Audit. During the audit, they shall specifically check and verify the AML/CFT procedure along with the forms/formats being used at the branches and comment on the lapses observed in this regard. The Internal Audit

shall scrutinize the entire AML/ CFT procedure adopted by the departments. A copy of such report shall also be provided to Compliance Department by Internal Audit.

6.2.4 Inspection by Compliance functionaries

Chief Risk and Compliance Officer himself/herself or compliance functionaries as assigned by him/her, may carry out onsite/ offsite inspection of the branches/extension counter with or without prior information to the concerned branch/extension counter. During the inspection, they shall assess the gap areas in regard to compliance of AML/CFT measures in addition to others and provide suggestion, feedback and guidance to the branch functionaries.

7. Key Elements of the Policy

The KYC, AML & CFT Policy of the Bank has the following key elements:

- Customer Acceptance Policy (CAP)
- Customer Identification Policy (CIP)
- Monitoring of Transactions
- Risk Categorization
- Training and Awareness of AML/ CFT Policy and Procedures
- Reporting

8. Customer Acceptance Policy (CAP)

Bank's Customer Acceptance Policy (CAP) lays down the guidelines for acceptance of potential customers and their beneficial owner and ensures that only those customers whose identity and purpose of opening accounts or performing transactions can be duly established and verified as legitimate are accepted.

Bank shall accept and open account in the name of natural person or any type of entities. The name shall have to be exactly the same and consistent with the one appearing in the identification document. No account shall be opened in the anonymous or fictitious name. Requisite information/documents shall be obtained from the customer for opening account or establishing business relation.

Customer appearing in the sanctioned list of OFAC, UN, EU or Nepal Government (published by Ministry of Home Affairs) shall not be accepted or business relationship with such person/ entity shall not be established or continued. Also, as per the provision mentioned in the Unified Directives issued by Nepal Rastra Bank (NRB) customers blacklisted by CIB are also not accepted.

Procedure of Customer Acceptance shall be described in the Procedural Guidelines on KYC, AML & CFT of the Bank.

9. Customer Identification Policy (CIP)

Customer identification means undertaking client due diligence measures while establishing business relation e.g. commencing an account-based relationship, but not limited to, including identifying and verifying the customer and the beneficial owners on the basis of the officially valid documents.

Customer identification requires identifying the customer and verifying his/her/their identity by using reliable, independent source documents, data or information. Thus, the first requirement of Customer Identification Policy (CIP) is to be satisfied that a prospective customer is actually who he/she claims to be. The second requirement of CIP is to ensure that sufficient information is obtained on the identity and the purpose of the intended nature of the banking relationship. This would enable risk profiling of the customer and also to determine the expected or predictable pattern of transactions. Customers need to be screened if they are Politically Exposed Persons (PEP) or family members or close associates of PEPs. Business relationship with such customers should be established or continued only with the approval of Senior management of the Bank. Customer Identification is applied to the customer as well as beneficial owner of the customer. Customer Identification requirements are different for different types of customers whether they are natural persons or entities.

The increasing complexity and volume of financial transactions necessitate that customer do not have multiple identities within a bank, across the banking system and across the financial system. This can be achieved by introducing a unique identification code for each customer. The Unique Customer Identification Code (CIF ID) will help banks to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. It would also make banking operations smooth for the customers. In this context, there shall be unique CIF ID for each customer, where all the accounts of the same customer should be tagged. A customer should not be allotted more than one CIF ID.

Required customer identification procedures along with due diligence have to be completed while establishing business relationship with a customer, Beneficial Owner, PEP & non-face to face customer.

If the provision regarding customer identification could not be applied for any new customer, account should not be opened, or business relationship should not be

established with such customer. In case of existing customer, business relationship must be terminated. If suspicious transaction/ activity is suspected, STR/ SAR should be lodged with FIU.

9.1 Identification of Beneficial Owner

As per the provisions stipulated under ALPA, ALPR and NRB Directives, the Bank shall have to identify beneficial owner while establishing business relation with customer or carrying out any transaction. It should be determined whether a client is acting on behalf of a beneficial owner. In addition to requirement of identifying beneficial owners of legal entities, the beneficial owner shall have to be identified even in case of natural persons where beneficial owner other than customer himself/herself exists.

The customer is also permitted to act on behalf of another person/entity, beneficial owner on following circumstances:

i) To represent individual for transactions/agreement within delegated authority by way of express documentary mandate in his/ her favour by the maker of such mandates and to the extent permitted by such mandates subject to laws of the land.

ii) To represent legal/fiduciary entities for transactions / agreements / arrangements with the Bank, within the express documentary delegated authority in his/ her favour by the maker of such mandate subject to laws of the land.

iii) To enter into transactions/ agreements with the Bank as directed by legislative/Executive/Judicial authorities to the extent and for the purpose specified by such authority.

iv) To enter into transactions / agreements with the Bank in respect of the individuals / entities as acceptable to the Bank in the light of prevalent banking laws and practices.

In case of legal entities/legal arrangements, ownership and control structure of the customer has to be determined and it should be identified who are the natural persons who ultimately control the legal entity. In general, following measures shall have to be applied to identify beneficial owners of legal entities/legal arrangements:

i) If there is any natural person, who owns or controls legal entity, such natural person shall have to be identified.

ii) If there is no such information or if there is uncertainty about the natural persons who own or control legal entity, it should be ensured whether there is any natural person or not who controls such entity.
iii) If there is no natural person that controls legal entity, key persons involved in the operation and management of such entity shall have to be identified.

Beneficial owners and the natural persons if any who control them, as mentioned below, shall have to be identified in case of legal entities/legal arrangements:

i) Natural persons that control or own the legal entity/ legal arrangement, directly or indirectly, by virtue of 10% or more share, other types of ownership, value or voting right or decision.
ii) Where 10% or more share of a legal entity is owned by other legal entity, all those natural persons who own 10% or more share of the other entity until the ultimate beneficial owner is identified.
iii) Natural person that has been involved in management or similar function of legal entity.
iv) Natural persons those may have control over legal entity.
v) In case of legal arrangement like trust, trustee, controller, protector, settler, beneficiaries and the natural person that control them.

While measuring effectiveness of indirect ownership or control of legal entity through natural persons, following standards should also be taken care of:

- In case of shareholder, partner of beneficiaries, their proportionate ownership.
- In case of control through family, proportionate ownership of family members.
- In case of control through other legal entities, proportionate ownership of partners, shareholders.

In case of legal entities listed on Nepal Stock Exchange, if their ownership structure/details, shareholding pattern, controlling interest, beneficiary details are published as per the law or if such particulars are easily available and if it is ensured from the reports that the entity has complied with international standards on AML/CFT, identification details of beneficial owners may not be necessary.

9.2 Customer Due Diligence

Customer Due Diligence is the process of identifying, verifying and evaluating customer and its beneficial owner on the basis of documents/ information provided by customer. After conducting Customer Due Diligence, money laundering and terrorist financing risk inherited with the customer can be identified. If CDD leads to a high-risk determination, the Bank is required to conduct Enhanced Customer Due Diligence.

9.3 Enhanced Customer Due Diligence

Enhanced Customer Due Diligence refers to additional due diligence of customer. Additional information pertaining to identity of the customer, source of income, nature, purpose and value of transaction etc. is obtained during ECDD. ECDD is conducted for high-risk customers or PEPs, if any unusual/ complex transaction is found or if any relationship with high-risk jurisdiction is found.

9.4 Simplified Customer Due Diligence (SCDD)

Simplified Customer Due Diligence (SCDD) is conducted to the customers posing lower risk of money laundering and terrorist financing. Nevertheless, there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances, it could be reasonable to apply Simplified CDD measures when identifying and verifying the identity of the customer and the beneficial owners.

9.5 Reliance on third party customer identification

For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, Bank may rely on a third party. However, Customer identification and verification may be executed through third party only if:

i) The Bank can ensure that the customer identification procedure is conducted by third party as per the standard AML/CFT norms to be followed by the Bank
ii) All the details, information and documents obtained for identification and verification of the customer is immediately available to the Bank.

However, The Bank shall not accept the customer identification and verification executed by third party if such third party is not regulated and supervised entity as per standard AML/CFT regime or if such party does not have adequate system in place for customer identification and verification as per standard AML/CFT norms or if such party is located at the jurisdiction of poor AML/CFT compliance or AML/CFT non-compliant jurisdiction.

Even in the case of third party customer identification and verification, ultimate responsibility of ensuring proper authenticity of information/documents lies with the branch maintaining such account.

9.6 Periodic Updating of KYC information

KYC information of the customers and beneficial owners have to be updated along with Customer Due Diligence and review of risk category for every customer on regular basis. KYC of customer should be updated in certain frequency. Irrespective of the frequency of periodic updating, KYC information of the customers and beneficial owners have to be updated immediately under following circumstances:

i) If transaction pattern is not commensurate with customer profile
ii) If customer identification procedure is not complete
iii) If the Bank has doubt over authenticity or veracity of KYC data, information or details obtained from the customer. If required

9.7 Suspension of KYC non-compliant accounts

Where the appropriate KYC measures could not be applied due to non-furnishing of information and/or non-cooperation by the customer, the branch shall suspend/ freeze the account after taking necessary steps to inform/ advise customer to update their KYC.

10. Monitoring of Transactions

KYC process does not end with opening of accounts. Monitoring of customer and transaction is an ongoing process. Transactions should be monitored depending on the risk sensitivity of the account. Branches/ Extension Counters should pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. In relation to the transactions requiring

special attention, background and purpose of the transaction should be tested in depth and conclusion of the findings shall have to be recorded in written form.

11. Risk Categorization

For proper risk assessment of business relationship with customers and evolving suitable monitoring mechanism, all new customers as well as existing customers are to be risk-categorized as High risk, Medium risk, Low risk and Lowest risk. Nature of customer, location/ geography of the customer or transaction, product/ service availed by customer and delivery channel used shall be the base for risk categorization of customer. Customer posing higher level of ML/ TF risk shall be categorized as high risk customers whereas customers with nominal level of ML/TF risk shall be the lowest risk customers. Enhanced Customer Due Diligence is to be applied for high risk customers whereas Simplified Customer Due Diligence is enough for lowest risk customers. Risk Categorizations done by the Branch should not be disclosed to the customers. Branch should ensure proper risk categorization of all customers and thereafter review at least in the prescribed frequency.

12. Training and Awareness of AML/ CFT Policy and Procedures

The Bank employees will conduct themselves in accordance with the highest ethical standards and the extant regulatory requirements and laws. Staff should not provide advice or other assistance to individuals who are indulging in money laundering activities. Ongoing employee training programmes should be conducted so that staff members are adequately trained in KYC/AML/CFT policy and procedures. All employees shall be provided with AML/CFT training at least once a year through direct or indirect means. The training modules/materials should be such that staff members are adequately trained in KYC/AML/CFT norms, policy, procedures and mechanisms.

For effective and result-oriented implementation of AML/CFT provisions as per ALPA, ALPR and NRB Directives, the bank shall arrange knowledge sharing programmes on AML/CFT for capacity enhancement of Board members, top management and shareholders having 2% or more share of paid-up capital at least once a year and at more frequent intervals upon requirement.

13. Reporting

13.1 Reporting to Financial Intelligence Unit (FIU- Nepal)

In terms of ALPA and NRB Directives, AML Compliance Officer is obliged to file following reports to the Financial Intelligence Unit-Nepal (FIU-Nepal) which has

been set up as a national unit, for interalia, collecting, analyzing, and disseminating information in respect of financial transactions:

i) Threshold Transactions Reports (TTRs)

Threshold Transactions Reports (TTRs) as prescribed by the regulator have to be filed to FIU within 15 days from the date of transaction through goAML portal.

ii) Suspicious Activity Report/ Suspicious Transaction Reports (SAR/STRs)

Suspicious Activity Report/ Suspicious Transactions Report (SAR/ STR) is required to be filed at the earliest within 3 days of reaching conclusion that the transaction is of suspicious nature through goAML portal. Suspicious Activity Report shall be filed if the activity/ behavior of the customer is suspicious, transaction may or may not take place and in case of attempted transaction also. Suspicious Transaction refers to the transaction of such nature that is impossible in general economic, commercial and business practice and the term also means similar other transactions, the FIU declares from time to time, as suspicious transaction. Amount of transaction does not matter for reporting suspicious transaction.

iii) Quarterly Report regarding AML / CFT

Quarterly Report regarding AML/ CFT where data of customers, KYC non-compliant customers, customer falling under different risk categories, STR, TTR, training etc. is to be reported in the prescribed format and submitted to FIU as well as Nepal Rastra Bank within 15 days from the end of each quarter.

iv) Details of Compliance Officer

Details of Managerial Level Compliance Officer appointed at Bank is to be reported to Financial Intelligence Unit (FIU-Nepal) and Bank Supervision Department of NRB. Name, address, qualification, contact number, email, etc. of Compliance Officer is to be communicated when Compliance Officer is changed and also if any information is changed.

13.2 Reporting to Nepal Rastra Bank (NRB)

Following reports shall have to be prepared and submitted to Nepal Rastra Bank.

- The AML CFT Report (Offsite Data Collection Form) as required by NRB will be prepared on half yearly basis i.e. every Ashad end and Poush end and will be submitted within 7 days from the end of each half of the year.
- AML/CFT Reporting Form (NRB 14) to be prepared and submitted to Bank Supervision Department, NRB on half yearly basis within 7 days from the end of each half of the year through Supervisory Information System (SIS).
- The AML CFT Reporting Format (Bank Self-Assessment Questionnaire) will be prepared on yearly basis i.e. every Ashad end and will be submitted within 15 days from the end of fiscal year through SIS.
- AML/ CFT Risk Assessment Report of the Bank is to be prepared and submitted to Bank Supervision Department of NRB within the first quarter from the end of fiscal year through SIS.
- Quarterly Report regarding AML/ CFT of the Bank is to be prepared and submitted to Bank Supervision Department of NRB as well as FIU Nepal within 15 days from the end of each quarter.
- Account blocked and released details is to be uploaded in SIS portal as and when any accounts are blocked or released as per the instruction of FIU, NRB and any other investigating and law enforcement agencies.

13.3 Counterfeit Currency Reporting

If any currency note or coin received from customers or any other parties at the branches/ extension counters is suspected to be counterfeit, it should be sent to Nepal Rasta Bank /Currency Management Department of Nepal Rastra Bank for their confirmation/verification along with Suspicious Currency Note Report, copy of deposit slip and depositor's Identity document (where available).

13.4 Reporting of information to various agencies/authorities

Nepal Rastra Bank, Department of Money Laundering Investigation (DMLI), Commission for Investigation of Abuse of Authority (CIAA), Courts, other investigating authorities, etc may issue order for freezing/unfreezing of assets/funds of the customer. Moreover, such authorities may also seek information/details of the customer in the course of investigation of money

laundering related crimes or any other crimes. Whenever, such freezing order or request for information/documents of the customer/transaction from such agencies/ authorities, which are competent to receive such information/details/documents as per the prevailing laws, is received, action should be taken immediately and the report/information/details should be furnished to the concerned authorities promptly, but not later than the prescribed timeline if any.

13.5 Reporting to Management/ Board level committees

Compliance status of KYC/ AML/ CFT guidelines should be presented to the Management Level committees as well as Board Level Committee in certain frequency. Assets (Money) Laundering Prevention Committee (ALPC) is the Board level committee constituted as per the provision of NRB Directives for oversight of AML/ CFT issues in the Bank. Reports are submitted to ALPC and ALPC further reports the status of compliance of KYC/AML/CFT guidelines as per the ALPA, ALPR, NRB Directives and Bank's policy on quarterly basis to the Board of the Bank.

14. Maintenance and Preservation of Records

Information and document related to customer and beneficial owner, information / document related to transaction, reports, conclusion of analysis and records shall have to be mentioned accurately and securely for minimum 10 years after termination of business relation with the customer or from the date of transaction or from the date of occasional transaction. In addition, such documents should be digitized and recorded so that same can be made available when required.

15. Correspondent Banking

Transactions conducted through correspondent banking relationships need to be managed taking a risk-based approach. "Know Your Correspondent" procedures should be established to ascertain whether the Correspondent Bank or counter-party is itself regulated for money laundering prevention and, if so, whether the correspondent is required to verify the identity of their customers. Correspondent Banking Relationship is established with the approval of Board of the Bank and Relationship Management Application (RMA) with the Bank can be established with the approval of Central Management Committee (CENMAC) of the Bank. Review of correspondent banks is to be

done during establishment of relationship and also on annual basis at least from AML/CFT perspective.

16. Wire Transfers

Banks use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

The salient features of a wire transfer transaction are as under:

i) Wire transfer is a transaction carried out on behalf of an originator person (natural person or legal entity) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.

ii) Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.

iii) Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.

iv) The "Originator" is the account holder/ beneficial owner of transaction, or where there is no account, the person (natural person or legal entity) that places the order with the bank to perform the wire transfer.

Bank shall ensure that complete information of sender as well as beneficiary along with the required document and information are obtained before initiating any transaction. In the process of wire transfer, the bank may be involved as ordering bank, intermediary or beneficiary bank.

i) Ordering Bank

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

ii) Intermediary Bank

For both cross-border and domestic wire transfers, a bank processing as an intermediary element of a chain of wire transfers must ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept at least for the period mandated by prevailing laws and same has to be made available to the beneficiary bank upon demand.

iii) Beneficiary Bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to FIU. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information of the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

17. Trade Based Money Laundering (TBML)

Trade-Based Money Laundering (TBML) is being rapidly growing around the world for the purpose of disguising proceeds of the crime and moving value through the use of trade transactions. It is the process by which criminals use a legitimate trade to disguise their criminal proceeds from illegal sources. Money laundering can be done through trade by under-invoicing, over-invoicing, misrepresentation of price, quantity, quality of traded goods. The Bank shall not be involved in TBML activities for which all the required process and procedures should be followed.

18. Combating of Financing of Terrorism

Combating of Financing of Terrorism, refers to a set of standards and regulatory systems intended to prevent terrorist groups from laundering money through the banking system or other financial networks. As per the provision of ALPA, Banks should immediately freeze the fund or assets of terrorist individual, group or organization published by Ministry of Home Affairs.

Moreover, in terms of Section 110 of the Banks and Financial Institutions Act, 2073, Nepal Rastra Bank may direct banks to freeze any account opened in the concerned licensed institution in the name of any individual, firm, company or institution in such a manner as to prevent the withdrawal or transfer of funds in any way from that account in connection with investigations into any type of crime or in connection with protecting the national interests by checking money laundering and terrorist activities or organized crimes.

Sanctioned Countries/territories are those countries/territories against whom the political and economic trade restrictions are put in place with the aim of maintaining or restoring international peace and security. Their principal purpose is usually to change the policies and actions of the sanctioned country's regimes, individuals or groups in a direction which will improve the situation in that country. It is also aimed at preventing weapons from falling into the wrong hands, disrupting terrorist operations and prohibiting the transfer of funds to a sanctioned country and freezing the assets of a government, the corporate entities and residents of the sanctioned country. Business relationship with such sanctioned jurisdictions is to be prohibited.

19. Proliferation of weapons

Proliferation Financing refers to the act of providing funds or financial services which are used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials that would contribute to the weapons of mass destruction proliferation (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. Proliferation is the illegal manufacture, acquisition development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials. 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 weapons of mass destruction.

20. Relationship with vendors, service providers and other parties

The Bank shall have to obtain relevant information/documents as deemed necessary for its relationship with vendors, service providers and other parties such as business partners, consultants, valuators, etc. All functionaries in the Bank will ensure at the time of approving outsourcing services that KYC/AML/CFT measures are implemented in letter and spirit and

no access is given to any individual/entity having direct/indirect link to banned entities/individuals.

21. Downward Correspondent Banking (Nested Account)

The Bank shall not provide/permit downward correspondent banking service and nested account activities to other financial institutions unless concerned correspondent bank permits/ provides consent for the same.

22. Payable-through Accounts (PTA)

The Bank will not provide customers with the services of payable through accounts i.e., direct access to any of its correspondent account held with foreign banks.

23. Introduction of New Technology

Bank will pay special attention to the money laundering threats arising from new or developing technologies and take necessary steps to prevent its misuse for money laundering activities. Bank will ensure that appropriate KYC procedures are duly applied to the customers using new technology driven products. Moreover, the bank shall assess the AML/ CFT risk and arrange for necessary procedure/ mechanism for managing the same while introducing any new technology, product or services.

24. Resubmission Policy

Once a transaction is rejected by Bank due to sanctions/money laundering/terrorist financing concerns, concerned department/branch shall maintain the record of such rejected transactions and shall not accept the same submitted by correspondent bank after stripping off information. Moreover, the Bank shall maintain record of the transactions rejected by correspondent bank and shall not attempt to resubmit same transactions after stripping off.

25. Tipping off & Confidentiality

The Bank will not share the information regarding unusual/ suspicious transaction, STR, TTR and correspondence to and from FIU, NRB, any investigating authorities with the customer or any irrelevant bank staffs, unrelated official meetings or anyone outside the bank. Doing so would constitute "Tipping Off", which is an offense prohibited by law. The bank is required to keep the documents, information and transaction details of the customer confidential and will not leak/share to unauthorized person.

26. Review of the Policy

This Policy will be reviewed at least once in a year incorporating the changes of regulatory provisions and findings of AML/ CFT Risk Assessment Report. However, it can be reviewed more frequently as and when considered necessary by the Board.

27. Authority to advise changes in the Interim period

Any other instructions under the policy, required to be issued urgently, before the review, may be issued with due approval from Managing Director & CEO. Any changes brought about by Government of Nepal / Nepal Rastra Bank or other regulators will be disseminated by way of circulars, under the signature of Managing Director & CEO or Deputy CEO.

28. Authority to issue clarifications

Authority to issue clarifications in all KYC/ AML/ CFT matters under this policy shall be Chief Risk and Compliance Officer.

****

Nepal SBI Bank Limited

Three Column Chart of revision of KYC, AML & CFT Policy of the Bank

The KYC, AML & CFT Policy of the Bank has been revised in the line of regulatory provisions incorporating amendment/ revision in internal policy/ structure of the Bank.

Major changes / revision/ amendment in the KYC, AML & CFT Policy of the Bank have been presented in the following chart:

Point/ Sub-point	Heading/ Sub-heading	Existing Provision	Revised Provision	Reason for Revision
6.1.3	**Operational Risk Management Committee (ORMC)**	Operational Risk Management Committee shall oversee the implementation of AML/CFT Policy and procedure of the Bank along with compliance of AML/CFT provisions as per ALPA, ALPR and NRB Directives. It shall analyze the gap if any in regard to compliance to AML/CFT provisions and provide suggestion, feedback and instruction for the compliance of the same.	Operational Risk Management Committee (ORMC) reviews operational risk related matter to mitigate the operational risk in Bank. AML/CFT related issues are also deliberated in the ORMC. It analyzes the gap if any with regard to compliance to AML/CFT provisions and provides suggestion, feedback and instruction for the compliance of the same.	Clarifying the roles and responsibilities of ORMC.
8	**Customer Acceptance Policy (CAP)**	Bank's Customer Acceptance Policy (CAP) lays down the guidelines for acceptance of potential customers and ensures that only those customers whose identity and purpose of opening accounts or performing transactions can be duly established and verified as legitimate are accepted	Bank's Customer Acceptance Policy (CAP) lays down the guidelines for acceptance of potential customers and their beneficial owner and ensures that only those customers whose identity and purpose of opening accounts or performing transactions can be duly established and verified as legitimate are accepted.	Customer Acceptance Policy applicable for Beneficial Owner also.
8	**Customer Acceptance Policy (CAP)**	-	Customer appearing in the sanctioned list of OFAC, UN, EU or Nepal Government (published by Ministry of Home Affairs) shall not be accepted or business relationship with	Inclusion of provision of NRB Directives

			such person/ entity shall not be established or continued. Also, as per the provision mentioned in the Unified Directives issued by Nepal Rastra Bank (NRB) customers blacklisted by CIB are also not accepted.	
9	**Customer Identification Policy (CIP)**	-	Customers need to be screened if they are Politically Exposed Persons (PEP) or family members or close associates of PEPs. Business relationship with such customers should be established or continued only with the approval of Senior management of the Bank. Customer Identification is applied to the customer as well as beneficial owner of the customer.	Customer Identification policy clarified
11	**Risk Categorization**	-	Nature of customer, location/ geography of the customer or transaction, product/ service availed by customer and delivery channel used shall be the base for risk categorization of customer.	As per the provision of NRB, basis for categorization of risk is clarified.
13.1	**Reporting to Financial Intelligence Unit (FIU-Nepal)** ii) Suspicious Activity Report / Suspicious Transaction Reports (SAR/STRs)	Suspicious Activity Report/ Suspicious Transactions Report (SAR/ STR) is required to be filed at the earliest within 3 days of reaching conclusion that the transaction is of suspicious nature. Such report is to be filed even if the activity of the customer is suspicious and actual transaction has not taken place and in case of attempted transaction.	Suspicious Activity Report/ Suspicious Transactions Report (SAR/ STR) is required to be filed at the earliest within 3 days of reaching conclusion that the transaction is of suspicious nature through goAML portal. Suspicious Activity Report shall be filed if the activity/ behavior of the customer is suspicious, transaction may or may not take place and in case of attempted transaction also.	Suspicious Activity Reporting is defined more precisely.
13.1	**Reporting to Financial Intelligence Unit (FIU-Nepal)** ii) Suspicious Activity Report / Suspicious	-	Amount of transaction does not matter for reporting suspicious transaction.	Suspicious Transaction Report is more clarified.

	Transaction Reports (SAR/STRs)			
13.1	**Reporting to Financial Intelligence Unit (FIU-Nepal)** iv) Details of Compliance Officer	Name, address, qualification, contact number, email, etc. of compliance Officer and compliance functionaries is to be communicated.	Name, address, qualification, contact number, email, etc. of Compliance Officer is to be communicated when Compliance Officer is changed and also if any information is changed.	Provision of NRB Directives incorporated.
13.5	**Reporting to Management / Board level committees**	Assets (Money) Laundering Prevention Committee (ALPC) should report to the Board the status of compliance of KYC/AML/CFT guidelines as per the ALPA, ALPR, NRB Directives and Bank's policy on quarterly basis. Compliance status of KYC/ AML/ CFT guidelines should also be put up to the Management Level committees in certain frequency.	Compliance status of KYC/ AML/ CFT guidelines should be presented to the Management Level committees as well as Board Level Committee in certain frequency. Assets (Money) Laundering Prevention Committee (ALPC) is the Board level committee constituted as per the provision of NRB Directives for oversight of AML/ CFT issues in the Bank. Reports are submitted to ALPC and ALPC further reports to the Board of the Bank the status of compliance of KYC/AML/CFT guidelines as per the ALPA, ALPR, NRB Directives and Bank's policy on quarterly basis.	Reporting process is more clarified.
15	**Correspondent Banking**	-	Correspondent Banking Relationship is established with the approval of Board of the Bank and Relationship Management Application (RMA) with the Bank can be established with the approval of Central Management Committee (CENMAC) of the Bank.	Approving authority is clarified as per the decision of Assets (Money) Laundering Prevention Committee (ALPC) of the Board.
Others:		• Minor clerical changes/ updates not included. • Only changed/ updated portion included in case of change/ update as mentioned above.		

****