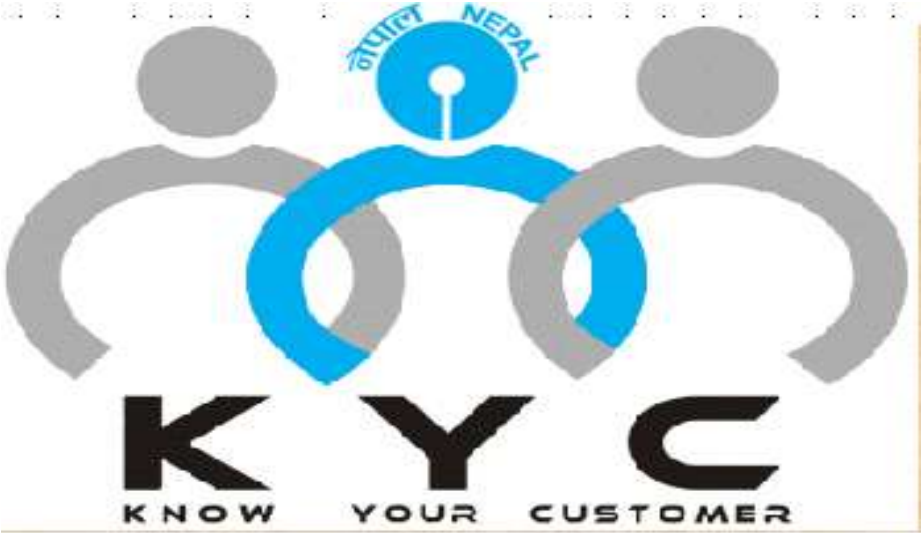
Policy and Procedural Guidelines on Know Your Customer (KYC), Anti Money Laundering (AML) and Combating of Financing of Terrorism (CFT)



Nepal SBI Bank Limited- 2011

First revision on 26.06.2014

Second Revision on…24.01.2017……

Table of Contents

Annexure

Preamble

Nepal Rastra Bank (NRB) has specified Know Your Customer (KYC) standards to be followed by Banks and Financial Intuitions (FIs) and measures to be adopted in regard to Anti Money Laundering (AML) and Combating of Financing of Terrorism (CFT).

Being a joint venture partner of State Bank of India (SBI), Nepal SBI Bank Ltd. (NSBL) is also required to adhere to the KYC/AML Policies and CFT measures of State Bank of India (SBI) as well.

THEREFORE, with a view to prescribe standards in respect of KYC and adopt measures to combat Assets Money Laundering and Combating of Financing of Terrorism, the Bank's Board of Directors has formulated these Policy and Procedural Guidelines in line with the "Assets (Money) Laundering Prevention Act, 2008", rules framed there-under and KYC/AML/CFT Directives of Financial Information Unit (FIU), Nepal Rastra Bank. The Policy also incorporates relevant standards and measures prescribed by SBI through its Policy and Procedural Guidelines on KYC, AML & CFT, to the extent of their applicability to NSBL as its foreign subsidiary.

1. Objectives, Scope and Application

The Primary objective of this Policy is to prevent the Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or financing of terror activities. Purposes proposed to be served by the Policy are:

a) To establish procedures to verify the bona-fide identification of individuals/ corporate bodies opening an account with the Bank.
b) To prevent criminal elements from using the Bank for money laundering activities
c) To enable the Bank to know/understand the customers and their financial dealings better, which in turn would help the Bank to manage risks prudently.
d) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
e) To monitor transactions for filing of Cash/Threshold Transaction Reports to FIU

f) To file counterfeit currency reports in cases of detection of counterfeit currency to NRB or appropriate authority.
g) To comply with applicable laws and regulatory guidelines
h) To ensure that the staff members concerned are adequately trained in KYC/AML/CFT laws, policies and procedures.

The focus of the KYC is for 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 identifying and keeping a watch on high value transactions and those of suspicious nature, as well as reporting them to Law Enforcing/ Regulatory authorities, as and when required.

This policy is applicable to all branches/offices of the Bank and is to be read in conjunction with related operational guidelines/circulars/office orders issued from time to time.

2. Definition of Know Your Customer(KYC) and Money Laundering

a) **"Know Your Customer" (KYC)** is the platform on which banking system operates to help control financial frauds, identify money laundering and suspicious activities, and for scrutiny and monitoring of large transactions. It is the documented guidelines 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. The policy 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.

It is also absolutely imperative to know clearly (a) the customer identity (b) the source of his wealth (c) the nature of his transactions. Proper documentation for the same should be a pre condition.

b) **Money laundering** 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 called money laundering.

Section 2 of the "Asset (Money) Laundering Prevention Act, 2008" (AMLPA), has defined the "offences of money laundering" as stipulated under chapter 2 of the Act, as under:

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

a) Converting and transferring property by any means knowing 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.
b) Concealing or disguising or changing the true nature, source, location, disposition, movement or ownership of property or rights with respect to such property knowing or having reasonable grounds to believe that it is proceeds of crimes.
c) 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.

Section 4 of the AMLPA prohibits "Terrorist Financing" as under:

(a) No person shall, by any means, directly or indirectly, unlawfully and willfully, provide or collect funds or assets with an intension that such funds or assets may be used or in the knowledge that they are to or intended to be used, in whole or in part, in order to carry out a terrorist act or by a terrorist or a terrorist organization.

In terms of Section 4 of AMLPA following acts also fall within the ambit of offense of terrorist financing:

- Any attempt to commit any act mentioned hereinabove.
- Providing or conspiring 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.
- Undertaking any of the following acts:

  (i) to participate as an accomplice in such act,
  (ii) to organize or direct others to commit such act,
  (iii) 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.
- If any of the following circumstances exist in relation to any act mentioned above, It shall be the offence of terrorist financing:
  i. Even if the terrorist act does not occur or is not attempted,
  ii. Even if assets or funds were not actually used to commit terrorist act or attempt thereof.
  iii. Even if such assets or funds are linked or not linked to a specific terrorist act,
  iv. Even if the terrorist act or intended terrorist act does occur or will occur in the same State or territory or somewhere else,
  v. Even if the terrorist organization and individual terrorist is or is not located in the same State or territory where the terrorist act is intended to or occurs,
  vi. Whether or not the assets or funds are collected or provided from legitimate or illegitimate source,
- Even if any act or offence mentioned above is committed in the foreign country or territory provided that the act is offence under the law of that state.

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.

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

3. Obligations under "Asset (Money) Laundering Prevention Act, 2008"

Section 7(P) & 7(R) of the Act, places the following obligations on the Bank:

(1) The Bank shall develop and implement AML/CFT Policy and Procedures compatible with its nation, geographic coverage, scope of operation, size of business, customer, transaction and risks for the prevention of money laundering and financing of terrorism and implement the Act, rules and directives thereunder, including the followings:

(a) Internal policies, procedures and controls relating to customer due diligence measures, information on transaction, verification, record keeping, monitoring, reporting and arrangement for regular monitoring

(b) Arrangement to implement obligations as per this Act, rules and directives thereunder,

(c) Adequate screening procedures to ensure high standards when hiring employees,

(d) Ongoing and refreshment training for employees,

(e) Independent and effective measures to review, verify, audit and update compliance of the Act, rules and directives,

(f) Measures for detection and information of suspicious transaction,

(g) Other measures as prescribed by the Regulator,

(h) Other measures to fulfill the obligations as per the AMLPA, rules and directives and other arrangement required for evaluation of effectiveness of the same.

(2) Bank shall have to appoint compliance officer of managerial level to comply the obligation pursuant to the provision of AMLPA or rules and directives issued. 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 Bank's records, books of accounts and documents related to financial transactions.

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

(c) Perform other necessary functions for implementation of AMLPA, rules and directives

(d) Perform other functions as prescribed by the regulator

(3) The Bank shall maintain records accurately and securely for minimum five years after the termination of business relationship or from the date of transaction in case of occasional transaction as under:-

(a) All documents and other information related to the 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) Documents and details of account and business relation of reporting entity,

(d) All documents and records relating to domestic and foreign transactions,

(e) Record and documents on attempted transactions,

(f) Other documents, details and records as prescribed by regulators.

(4) The Bank shall keep some prescribed documents and records for more than five years securely.

(5) The Bank shall keep and maintain documents and records mentioned above in such a way that it shall be sufficient to reconstruct such information for the use of legal action as evidence.

(6) The Bank shall keep the report of suspicious transaction for five years.

(7) Documents and records should be kept in such way that it could be made readily available to competent authorities upon demand.

4. Risk Perception

Non compliance with KYC/AML/CFT standards/measures can lead to use of the technology channels of the Bank for Money Laundering/financing terrorism activities and thus expose the

Bank to various risks such as Operational risk, Reputation risk, Compliance risk and Legal risk, etc.

5. Key Elements of the Policy

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

- Customer Acceptance Policy
- Customer Identification Procedures
- Monitoring of Transactions and
- Risk Management

6. Customer Acceptance Policy

Bank's Customer Acceptance Policy (CAP) lays down for acceptance of customers.

6.1 Definition of Customer

A customer for the purpose of these guidelines is defined as:

(i) A person or an entity that maintains an account and/or has a business relationship with the Bank (including borrowers and guarantors of loans sanctioned by the bank, Demat account holders, Locker holders, etc.)

(ii) One on whose behalf the account is maintained i.e. the beneficial owner, described in paragraph 7.4(c) hereunder.

(iii) Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, lawyers etc., as permitted under the law, and

(iv) Any person or entity connected with a financial transaction with the Bank.

6.1.1 A customer of the Bank is permitted to act on behalf of another person/entity, beneficial owner, in the following cases:

(i) To represent individual for transactions/agreement within delegated authority by way of express documentary mandate in his 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 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.

6.2 Customer Acceptance

6.2.1 The guidelines in respect of the customer relationship in the bank, broadly, are:

i. No account is to be opened in anonymous or fictitious/benami name(s)/entity (ies). In other words, thorough checking of antecedents to avoid opening of accounts in fictitious/benami names.

ii. Accept customers only after verifying their identity, as laid down in Customer Identification Procedures (discussed later in Chapter 7.1).

iii. Not to open an account or close an existing account (except as provided in Chapter 8.6 hereinafter), where identity of the account holder cannot be verified and/or documents/information required could not be obtained/confirmed due to non-cooperation of the customer.

iv. Identity of a new customer to be checked so as to ensure that it does not match with any person with known criminal background.

v. Classify customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of customers. Also, a profile of each customer will be prepared based on risk categorization.

vi. Documentation requirements and other information to be collected as per Asset (Money) Laundering Prevention Act, 2008 and Rules/Guidelines/Directives framed

there-under by Government/NRB/FIU and Bank's guidelines/instructions are to be complied with.

vii. Accounts of persons having relationships with banned entities such as individual terrorists or terrorist organizations etc. are not to be opened. While information relating to them will be shared from time to time, branches will also have to be guided by the information available in public domain for the purpose.

viii. Further, accounts should not be opened for persons convicted for predicate offences such as money laundering, terrorist activities, drug trafficking, bank frauds, immoral trafficking etc. List of various types of predicate offenses under prevailing laws are listed under Annexure G.

ix. Accounts of persons, who have been convicted, are lodged in jails, can be opened with suitable safeguards decided on case to case basis, jointly with the superintendent of the respective jail, with a view to ensuring financial inclusion, provided such persons have not been punished for predicate offences. However, it should be ensured that banking facilities are not denied, for genuine purposes, merely for the reason that criminal charges have been leveled against them or they have undergone some form of punishment in the past.

6.2.2 It is important to bear in mind that the adoption of Customer Acceptance Policy and its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

7. Customer Identification

7.1 Customer Identification Requirements

Customer identification requires identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Thus, the first requirement of Customer Identification Procedures (CIP) to be satisfied is 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.

While verifying KYC documents, care should be exercised to ensure that one specific ID document like Citizenship Certificate, National ID Card, PAN card, passport, registration certificate etc is not permitted to be used for opening accounts in various names and styles especially under proprietorship. This will preclude the possibility of any forged/illegal document being used for opening several types of accounts. Similarly, extra care should be taken while opening accounts of various firms and companies belonging to the same group accounts and under no circumstances accounts of shell companies/firms should be opened in the Bank's books.

Note: Shell Company/firm means a company/firm that has no independent assets or operations of its own, but is used by its owners to conduct specific business dealings or maintain control of other companies

Identification data, as under, will be required to be obtained in respect of different classes of customers:

7.1.1 For customers that are Natural persons:

a) Address/location detail.
b) Recent photograph/proof of identity.

7.1.2 For customers that are legal persons:

a. Legal status of the legal person/entity through proper and relevant documents
b. Verification that any person purporting to act on behalf of the legal person/entity is so authorized and identity of that person is established and verified
c. Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person

Wherever applicable, information on the nature of business activity, location, mode of payments, volume of turnover, social and financial status etc, will be collected for completing the profile of the customer.

7.1.3 List of KYC Data/Documents to be obtained from different categories of customers for verification of their identity and address is shown as annexure A to this Policy/Guideline.

7.2 Customer Identification Stages and measures

A) The customer Identification Procedures are to be carried out at the following stages:

- While establishing a banking relationship;
- While opening an account
- When the bank feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account.
- Customer identification data (including photograph/s) should be periodically updated after the account is opened. Such verification should be done at least once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk customers.
- Customer Identification will also be carried out in respect of non-account holders approaching bank for high value one-off transition as well as any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Bank.
- While making frequent transactions below the threshold limit
- While making electronic fund transfer.
- When the bank found a person involved in suspicious transaction or act
- When additional verification is required in case there is suspicion of money laundering or terrorist financing
- At any time of transaction in relation to the high risk and politically exposed person,

B) The Bank shall adopt following measures to undertake proper identification and verification of its customers:

- To obtain suitable information and disclosure regarding transaction or business relation and purpose or intended nature of business of the customers.
- If the customer is a natural person, to obtain particulars including name, address and date of birth interalia based on the documents prescribed under 7.3.1(a) herein.

- If the customer is an artificial person or legal arrangement, to obtain information and disclosure and verify its ownership and control structure.
- When a person is establishing business relationship or conducting transaction on behalf of another customer, obtaining identification document of such person and the person working on behalf of him/her including evidence verifying that that such person is properly authorized to act.
- To obtain other information and details regarding customer, transaction and its nature.
- To adopt other measures as prescribed by the regulators from time to time.

C) Not to Carry out Transaction: The Bank shall not open a bank account or continue business relationship or conduct transaction with the following customers:-

(i) Customer who cannot provide documents, information and details required for the customer identification and verification process defined herein

(ii) Documents, information and details provided appear conflicting to the identity of the customer

(iii) Individual or entity listed in the sanction list of the Department of Money Laundering Investigation, Government of Nepal, United Nations, OFAC, etc.

Letters of Thanks in all instances of opening of new accounts to be sent by registered post or courier at the recorded addresses to all customers and introducers with dual purpose of thanking them for opening the account with the Bank and for verification of genuineness of address furnished by the account holder. Undelivered envelopes in this regard would be required to be followed-up closely at branch/ Corporate Office level and proper noting is to be made in the formalities register at the branches. Copies of letters are to be kept on record.

When signatories change, care should be taken to ensure that the identity of any new signatories has been verified as laid down in chapter 7.1 above.

7.3 Customer Identification Procedure

7.3.1 Accounts of Individuals:

The customer identification will be on the basis of documents provided by the customer as (a) Proof of identity and (b) proof of address. Prescribed application form along with recent Photographs of the customer is to be invariably obtained in all cases.

(a) Proof of identity: Proof of identity (any of the following, with authenticated photographs thereon)

(i) Nepali Citizenship Certificate or National ID Card
(ii) Passport*
(iii) In the case of Refugees; Refugee Identity Card issued by Government of Nepal or UNHCR.

[*In the case of Indian nationals, Certificate of Registration of Indian National issued by Embassy of India (EOI)]

Documents accepted for proof of identity should be verified through public/concerned authority's website wherever such information is available online.

(b) Proof of address: Any one or more of the following evidencing permanent and residential address:

(i) Migration Registration Certificate
(ii) Land Ownership Registration Certificate (Lalpurja)
(iii) PAN Card
(iv) Salary slip
(v) Income/Wealth Tax Assessment Order
(vi) For the applicant residing on rent; name, address and phone no of the house owner and, if possible, copy of lease agreement.
(vii) Bank account statement
(viii) Letter from reputed employer
(ix) Letter from any recognized Government authority having proper and verifiable record of issuance of such certificates.
(x) Voter ID card (only if it contains the current address)

(xi) Pension Payment Orders issued to retired employees by Government Departments and Public Sector undertakings, if they contain current address.

(xii) Copies of Registered Leave & License agreement/Sale Deed/Lease Agreement may be accepted as proof of address.

(xiii) Certificate and also proof of residence, incorporating local address as well as permanent address, issued by the Government authority/college/University/Reputed Employer. For students residing with relatives, address proof of relatives, along with their identity proof, can also be accepted provided declaration is given by the relative that the student is related and is staying with him/her.

(xiv) In respect of close relatives e.g. wife, son, daughter and parents etc. who live with their husband, father/mother and son/daughter, as the case may be Branch can obtain an identity document and a utility bill of the relative with whom the prospective customer is living, along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her. However, in case of joint accounts, applicants who are not closely related to each other would be required to establish their identity and address independently

(xv) If the applicant is an employee of the Government of Nepal or Public Sector Undertakings or teachers/professor or employee of the Government funded institutions/college/school/universities, a copy of photo identity document.

(xvi) If the applicant is a practicing professional like lawyer, auditor, chartered accountant, engineer, doctor, etc., a copy of license issued by the competent authority.

(xvii) For the applicant residing on rent; name, address and phone no of the house owner.

Documents accepted for proof of address should be verified through internet using public/concerned authority website wherever such information is available online.

The Identity of the Customer also needs to be verified by at least one of the introducers prescribed by the Bank as eligible introducer as per Annexure-B.

7.3.2 While the above set of documents should normally suffice to establish both the identity and the correct address of the applicant, wherever this is not so (e.g. PAN card and salary Slip together may not provide proof of address) applicants to be asked to give additional documents e.g. a letter from the employer giving the correct address, credit card statement etc. While accepting identity documents which are not issued by Govt. Agencies/ public Sector Agencies, branches should endeavor to obtain at least one document like PAN Card, Voter ID Card, Migration Certificate, Land Ownership Registration Certificate, passport etc. which has been issued by public Authorities after completing independent due diligence.

7.3.3 Whenever request for change of address is received, address verification procedure should be adhered to and change of address should be effected only after such verification and documents indicating revised address be kept on record.

7.3.3.1 Special Provisions for Identification of Politically Exposed Person (PEP), family members and associated persons of PEP:

(1) The Bank shall adopt Risk Management System to screen its existing as well as potential customers and their beneficial owners to identify their status as Politically Exposed Person (PEP) and/or family members and/or associated person of PEP.

(2) As regards any business relation with the domestic or foreign PEP, their family members and individuals associated with PEP, the Branches will adopt additional measures as under:

(a) To establish business relation with such customers only with the prior approval of the officer one stage higher than the authorized official or Regional Manager where the Branch Manager is the authorized official. Approval for continuation of business relation from Competent Authority/ RM shall also be obtained when any existing customer is known as PEP or their family member or associated with PEP.

(b) To take all reasonable measures to identify the sources of fund and assets of such customers or beneficial owner. To satisfy this requirement the Branches may obtain documents evidencing sources of funds/asset (e.g.,

copy of tax clearance certificate, sell/purchase deed (Rajinama), salary sheet, pension proof, contract paper, etc.) or obtain customer's declaration in regard to legitimacy of the sources of funds/assets. Further, proof of identity (as mentioned in Point No. 7.3.1 (a) of this policy) of all members including minors of undivided family of such customer should be obtained.

(c) To monitor the transaction/business relationship of such customers on an ongoing basis.

(d) To conduct Enhanced Customers' Due Diligence (CDD), at least once in 6 months.

7.3.3.2 Beneficial ownership to be identified:

(1) The Branches shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner before establishing business relationship or conducting transaction with any customer.

(2) The Branches shall take all reasonable measures to ascertain whether a person is acting or establishing business relationship or conducting transaction, on behalf of another person.

7.3.4 KYC Compliance for existing Accounts:

All the accounts to be opened henceforth as well as the accounts opened prior to issuance of this Policy are required to be fully KYC compliant in terms of this Policy. In case, there are any gaps, these should be filled on an urgent basis and confirmation to this effect must be submitted by the Branches to the Chief Risk and Compliance Officer, Corporate Office within 15 days from the date of issuance of this Policy through Compliance Officer of the Bank. The guidelines stipulated herein are equally applicable to one off transactions like remittances, new technology initiatives like online banking, debit cards, correspondent transactions, wire transfers, NEFT, RTGS, etc. as well.

7.3.5 Customer Due Diligence:

The Branches/Offices should undertake Customer Due Diligence (CDD) measures when:

a. Establishing business relationship.
b. Carrying out occasional transactions above the applicable designated threshold for the account.
c. This also includes where the transaction is carried out in a single operation or in several operations that appear to be linked.
d. Carrying out occasional transactions that are wire transfers on any other mode like RTGS, NEFT, SWIFT etc.
e. There is a suspicion of money laundering or terrorist financing, regardless of any exemptions or thresholds that are referred to elsewhere.
f. The Branch/Office has doubts about the veracity or adequacy of previously obtained customer identification data.

7.3.6 Enhanced due diligence is required to be exercised when establishing business relationship or conducting transaction with the following customers:-

(a) Customer identified as high risk

(b) Customer who conducts complex, unusual large transactions and unusual patterns of transactions or which have no apparent economic or visible lawful purpose,

(c) Transaction with customer of a country, which is internationally, identified as a deficient or non-compliant country of international AML/CFT standards,

(d) PEP, his/her family member and person associated with PEP,

(e) Customer consuming high risk products and services,

(f) Customer suspected of ML, TF or other offence

(g) Other customers as prescribed by the Regulator.

7.4 Customer identification requirements- Indicative Guidelines

a. Trust/Nominee of Fiduciary Accounts:

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures.

Branches/offices should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, branches/offices should insist on production of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place.

While opening a Trust account, branches/offices should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), guarantors, protectors, beneficiaries and signatories. In the case of a 'foundation' or non-governmental organization registered under the Organization Registration Act, 2034, steps should be taken to verify the founders/members/office-bearers//directors and the beneficiaries.

b. Accounts of Companies and Firms

Branches/Offices need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with the Bank, they should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a listed public company it will not be necessary to identify all the shareholders. However, directors, partners, trustees, shareholders as significant owners (≥ 10%) should be subjected to KYC norms. In terms of extant guidelines, KYC compliance in respect of all these individuals is to be ensured in addition to applicable KYC compliance on legal persons.

Details of registration of companies should be verified through official website of the Office of Company Registrar, Tripureshwor, Kathmandu, Nepal, www.ocr.gov.np, wherever available, in addition to verification of copies of KYC documents from the originals thereof. Further, PAN details of the firm/company should be verified through official website of the Inland Revenue Department, Lazimpat, Kathmandu, Nepal, www.ird.gov.np/PanSearch. Money Laundering Reporting Officers (MLRO) are required to keep duly stamped web generated copy of verification of company registration (where applicable) and PAN of the firm/company, the stamp should consist of date of visit of website and name and signature of visiting officer.

Branches should examine the control structure of the entity, determine the source of funds and identity of the persons who have a controlling interest and who comprise the management with

a view to guard against entering into relationship with business entities being used by individuals as a 'front' for maintaining accounts with the Bank.

c. Client Accounts opened by professional Intermediaries

When the Branch/Office has knowledge or reason to believe that more than one client accounts have been opened by a professional intermediary on behalf of a single client, it has to carry out investigation to identify such accounts. Branches/Offices may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branches/Offices also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the Branches/Offices and there are 'sub-accounts', each of them attributable to a beneficial owners must be identified. Where such funds are co-mingled at the Branch/Offices, the Branches/Offices should still look through to the beneficial owners. Where the Branches/Offices rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. **It should be understood that the ultimate responsibility for knowing the customer lies with the Bank.**

d. Accounts of Politically Exposed Person *(PEPs) and their family members and close relatives.*

"Politically exposed person"(PEPs) means any domestic PEP or foreign PEP or international organization PEP and the term shall also denote the person categorized as PEP by Nepal Government in recommendation of National Coordination Committee by publishing notice in Nepal Gazette.

Politically Exposed persons are individuals who are or have been entrusted with prominent public function in the country or abroad, e.g. Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state owned corporations, important political party officials, etc.

Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Branches should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Such accounts should be subjected to enhanced monitoring on an ongoing basis. The above norms should also be applied to the accounts of the family members and close relatives of PEPs.

e. Accounts of Non-face to face Customers

Non face to face customers are those with whom the Branch has not had direct interaction at the time of opening the account- customers who opened the account without visiting the Branch. Branches/Offices are instructed to avoid opening of accounts of such customers as a general rule. Exceptionally they may accept verification of documents by officers of correspondent banks whose signatures are verifiable through one of the branches of the Bank.

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face to face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, Braches/Offices may also require the first payment to be effected through the customer's accounts with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place as responsibility for correctness of identity/residence proof lies with the branch monitoring such account or handling one off transaction.

f. Accounts of Minors

All KYC norms and procedures applicable for a natural person are equally applicable for opening the account of a minor, as the minor himself/herself cannot operate the account, ID proof of the person who will operate the account is also to be obtained. In addition, all KYC norms and procedures are to be fulfilled on the guardian of the minor as well.

7.5 Correspondent Banking

Transactions conducted through correspondent 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 as per Financial Action Task Force (FATF) standards. Where this is not the case, additional due diligence will be required to ascertain and assess the correspondent's internal policy on money laundering prevention and its Know Your Customer procedures. Accounts of correspondents will be terminated, after giving notice, if they fail to provide satisfactory answers to reasonable questions including, where appropriate, confirming the identity of customers featuring in unusual or suspicious activity / transactions. Shell Banks are not permitted to operate in Nepal therefore no correspondent relationship should be established with a Shell Bank. Bank should exercise due diligence at the time of establishing new correspondent relationship and also at the time of reviewing/renewing such relationships, especially from AML/CFT angle. Bank's Treasury Department, Corporate Office will complete AML/CFT compliance test for all the existing Banks/Financial Institutions with which the Bank has correspondent relationship in the format prescribed in Annexure F, within 3 months from the end of each fiscal year.

7.6 Authority Structure for KYC/Compliance

The officer-in-charge vested with the authority to open the account, should ensure compliance with the KYC guidelines. The employee/officer, who has interviewed the customer should subscribe his/her signature, in the space provided in the CDD form prescribed in Annexure-D of this Policy, for having interviewed the prospective customer and should ensure that all aspects of KYC guidelines are complied with.

7.7 Customer Profile

For the purpose of monitoring individual transactions in accounts, "Customer Profile" of individual account holders should be compiled in the account opening forms, covering the following information:

(i) Occupation
(ii) Source of funds
(iii) Monthly Income
(iv) Annual turnover
(v) Date of Birth
(vi) Educational qualification
(vii) Details of existing credit facilities, if any
(i) Details of Assets (approximate value).
(ii) Details of Other Accounts maintained with the Bank (if any), Customer profiles to be prepared for all accounts.

Customer profiles have to be reviewed whenever the branch/office has doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

Accounts opened in one Branch/Office should not be transferred to other Branch/Office. In case any account is required to be transferred for any reason, the customer profile should be updated by the Branch/Office where the account is transferred. While converting any inactive, inoperative and dormant account into live ledger, it should be ensured that KYC Guidelines are complied with.

Additional Information to be collected for Risk Categorization:

a) Purpose/reason for opening the account or establishing the relationship
b) Anticipated level and nature of the activity that is to be undertaken
c) Expected source of funds
d) Details of occupation / employment and sources of wealth or income.

7.8 Care to be Exercised

- Introduction of large number of accounts by a single introducer – either Existing account holder or Eligible Introducer as per Bank's Operation Manual (other than an employer company or institution) - to be probed thoroughly.
- The information collected from the customer at the time of opening account will be treated confidential and not be used or divulged for cross selling.
- Customers availing Internet Banking facility and other New Technology products also should be subjected to KYC measures.

7.9 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.

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

a) Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) 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.

b) 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.

c) 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.

d) The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

ii. Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their

assets. The information can be used by Financial Information Unit - NRB (FIU-NRB) for analysing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-NRB. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits.

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

(A) In Cross-Border Wire Transfers

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

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

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

d) All cross-border wire transfer of Rs.50,000 (Rupees Fifty Thousands only) and above is effected only by debit to customer's account or against cheques/drafts and not against cash.

(B) In Domestic Wire Transfers

a) Information accompanying all domestic wire transfers of Rs. 75,000.00 (Rupees Seventy Five Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means. It should further include name and account number (where account number is not available unique reference number for identification of transaction) of the beneficial owner.

b) If a bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs. 75,000/- (Rupees Seventy Five Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be submitted to FIU-NRB. Customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be submitted to FIU-NRB.

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

(iii) Exemptions

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

(iv) Role of Ordering, Intermediary and Beneficiary

(a) Ordering Bank

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

(b) Intermediary Bank

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

(c) Beneficiary Bank

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

8. Risk Categorization

For proper risk assessment of business relationship with customers and evolving suitable monitoring mechanism, all new customers are to be categorized as High risk, Medium risk and Low risk. It is to be specifically noted that risk categorization is meant for proper monitoring of accounts and does not reflect in any way on the account holders. **Risk Categorizations done by the Branch should not be disclosed to the customers.** While the extent of knowledge / information available on customers to prove their identity sufficiently will determine the risk perception and concomitantly risk categorization.:

Branch should ensure that risk categorization of all customer accounts is completed expeditiously and thereafter reviewed at least once six months. Following benchmarks have been finalized for facilitating risk categorization of all accounts as well as standalone transactions in the Bank. Branches/Extension Counters/Offices should complete the form as per 'Annexure D' at the time of opening the account and every time the account is reviewed thereafter and keep the same in the File of the Customer.

We give below an illustrative list of Accounts/ customers / groups who may be assigned different risk categories:

8.1. Low Risk (Category "A")

Accounts of:

i. Salaried employees / pensioners whose income structures are well defined
ii. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
iii. Other Individuals with debit or credit summations below Rs.10 lacs p.a. (For existing accounts, summation for last year will be considered and for new accounts, projected level will be considered).
iv. Small Business Enterprises and Public Limited Companies with debit or credit summations below Rs.10 lacs p.a. (For existing accounts, summation for last year will be considered and for new accounts, projected level will be considered).
v. *Government Departments and Government owned Companies, Regulators, FIs, Statutory Bodies, etc.*
vi. All borrowal accounts other than those classified as High Risk and Medium Risk.
vii. All such customers as classified by FIU-NRB as Low Risk.
viii. All deposit and borrowal accounts pertaining to the Government of Nepal, Governmental Bodies/Corporations/ Companies/Organizations, JVs with Govt., Regulators, FIs, and Statutory bodies may be classified as Low Risk accounts.
ix. Borrowal accounts, if the annual turnover in the accounts falls within the following parameters :-

    a. Working Capital Loans of any type -10 times of FBL
    b. Project Loan- 15 times of monthly installment
    c. Personal Overdraft- 10 times of limit
    d. Loan repayable in EMI- 15 times of monthly EMI
    e. Loan against FD, NSB, Approved Gov. Bond, etc.- 10 times of limit

x. Borrowal accounts, other than NPA accounts, having credit limit upto Rs. 1 crore

xi. All office accounts Inter Office Accounts, accounts of Banks/FIs

8.2 Medium risk (Category-"B")

Accounts of:

i. Individuals and persons engaged in Business.*
ii. Firms in private sector, Private Limited companies, etc.*
iii. Public Limited Companies*
iv. Individuals, firms, companies or organizations classified by FIU-NRB as Medium Risk or Risk Account
v. v. All borrowal accounts having borrowal limits above Rs. 1 crore and upto Rs.10 crores may be classified as Medium Risk.
vi. vi. All accounts having more than 60% forex remittance transactions may be classified as Medium Risk
vii. All dormant/inoperative accounts may be classified as Medium Risk.

** with Debit or Credit summations of Rs.10 lacs to Rs.1 crore p.a. (For existing accounts summation for last year will be considered and for new accounts projected level will be considered).*

8.3 High Risk (Category-"C")

i. Accounts of firms in private sector, Private Limited Companies and individuals with Debit or Credit summations above Rs.1 crore p.a. (For existing accounts summation for last year will be considered and for new accounts projected level will be considered).
ii. All account of Customers domiciled in high risk countries as categorized by FATF and updated by FIU/Home Ministry from time to time.
iii. Trusts, charities, Non Profit Organizations, NGOs and organizations receiving donations from Nepal and abroad.
iv. Politically Exposed Persons (PEP)s of the Country or aboard.
v. Non-face to face customers
vi. Those with dubious reputation.

vii. Borrowal accounts which are NPAs.

viii. All other customers who do not fall in Category 'A' and 'B'.

ix. All other accounts classified by FIU-NRB as "High Risk Account".

x. All non face to face deposit accounts, including NRN accounts, will be classified as High Risk.

xi. Borrowal accounts having limits of Rs. 10 crores and above will be classified as High Risk.

xii. Accounts having more than 75% forex remittance transactions to be classified as High Risk.

xiii. All accounts of Trusts, NGOs, Charities and Organizations receiving domestic or foreign donations and accounts operated by Power of Attorney holders may be classified as High Risk.

xiv. All accounts in the name of Politically Exposed Persons (PEPs) of foreign origin and individual/entities involved in any fraud/forgery/antinational activity/terrorism/tax evasion/insider trading may be classified as High Risk.

8.4 Care to be taken when categorizing the account

Branch should ensure that risk categorization of all customer accounts is completed expeditiously and care to be taken when categorizing the account in the following manner:

a. New accounts, except those pertaining to Governmental Bodies/ Corporations/ Companies/ Organizations and JVs with Govt., Regulators, FIs, Statutory bodies, salaried persons employed with the above organizations and pensioners from these organizations, will be classified as Medium Risk during the first year of operation unless they can be categorized under specific risk category based on the benchmarks mentioned herein above from point No. 8.1 to 8.3 and at other parts of this policy.

b. All deposit accounts of salaried persons, pensioners, households, students may be classified as Low Risk provided the turnover is upto 15 times monthly income or Rs. 10 lacs, whichever is higher.

c. All deposit accounts of agriculturists, rural artisans, labourers, having only domestic credits/debits may be classified as Low Risk provided debit/credit summations in the account do not exceed Rs.10 lacs p.a. or 15 times monthly income, whichever is higher.

d. Deposit accounts mentioned in (b) and (c) above, where the transaction value is higher than the specified threshold levels but below Rs. 1.00 crore per annum will be classified as Medium Risk accounts. Accounts having turnover of Rs. 1.00 crore and above per annum should be classified as High Risk accounts.

e. All accounts in Low Risk category may be moved to Medium Risk to High Risk category on exceeding the transaction of 50-75% of the respective threshold for Low Risk is undertaken in an account, the account will be classified as Medium Risk. Similarly, if a single transaction is for 75% or more of the threshold level, the account will be categorized as High Risk.

f. In respect of foreign inward remittances and commercial remittances, risk parameters and monitoring will be required to be done by Central Operations Department, Corporate Office.

g. In respect of Locker holders, the customer availing locker facility shall also be categorized into low, medium and high risk based on the category of the customer account associated with the locker facility. It should further be identified if the customer availing locker facility is domestic or foreign politically exposed person, their family members or associated persons. Procedure and frequency of customer due diligence and review of the risk category of the locker holder will be as applicable to the customer account.

h. Simplified Customer Due Diligence (CDD):

The general rule is that customers must be subject to the full range of Customer Due Diligence (CDD) measures, including the requirement to identify the beneficial owner. 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 owner.

Examples of customers or transactions where simplified CDD measures could apply are:

(i) Bank and Financial Institutions Licensed and supervised by Nepal Rastra Bank
(ii) Saving and current account having annual turnover of less than Rs. 1.00 lacs.
(iii) Public companies listed with the stock exchange regulated by Securities Board of Nepal

(iv) Foreign public companies which fulfill all of the following requirements:

- Listed with foreign stock exchange recognized by Financial Information Unit
- Regulated and supervised under the appropriate disclosure mechanism.
- Located at the territory which is fully compliant with international standards on AML/ CFT norms.

(v) Foreign Financial Institutions which fulfill all of the following requirements:

- Licensed, regulated and supervised under the mechanism established to combat money laundering and terrorist financing in consistent with the International standards
- Not questioned or penalized on the ground of violation of international standards on combating of money laundering and terrorist financing
- Located at the territory which is fully compliant with international standards on AML/ CFT norms.

While determining fully compliant status, with international standards on AML/ CFT norms, of the territories or countries of non- resident and foreign companies as mentioned in (d) & (e) above, the list or report published by Nepal Rastra Bank and the information/report published on the website of FATF, APG, IMF, World Bank are to be taken into consideration.

Notwithstanding anything contained hereinabove, simplified customer due diligence measures should not be applied for the customers of the territories or countries that are informed to be non-compliant with international standards on combating of money laundering and terrorist financing through any of following means:

- Informed by Nepal Rastra Bank or
- Identified by the Bank itself through reliable independent sources or
- If there is adequate doubtful grounds for such risk thereof for any reason whatsoever.

For the customers as mentioned hereinabove, customer acceptance policy, customer identification requirement and the procedure of due diligence will be the same as applicable to other customers. However, risk categorization shall be reviewed not less than once in 12 months till the customers meet the requirements as mentioned hereinabove.

8.5 Transactions Requiring Special Attention

It is important to recognize that the KYC process does not start and end with opening of accounts. Transactions should be monitored depending on the risk sensitivity of the account. Branches should pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the branch functionaries. High risk accounts should be subjected to intensive monitoring. High value transactions by non account holding customers also need to be monitored carefully.

8.6 Closure of Accounts

Where the appropriate KYC measures could not be applied due to non-furnishing of information and/or non-cooperation by the customer, the account can be considered for closure or terminating the banking/business relationship. Before exercising this option, all efforts will be made to obtain the desired information and, in the event of failure, due notice, will be given to the customer explaining the reasons for taking such a decision. The competent authority to permit closure of such accounts shall be the Branch Manager/Officer-In-charge where the Branch Manager/Officer-In-charge concerned is Assistant Manager Level or above. In all other cases, designated Regional Manager or the Chief Financial Officer in direct reporting branches/entities shall be the competent authority to permit closure of such accounts. Further, in case of non-cooperation by the customer for making his account KYC compliant, Suspicious Transaction Report should be filed by the Branch to the Compliance Officer, Corporate Office.

9. Monitoring of Transactions

A dedicated Compliance Cell for the entire Bank has been established at Corporate Office under the control of the Chief Risk and Compliance Officer.

The Compliance Cell will be headed by at least Managerial level official who will report to the Chief Risk and Compliance Officer (CRCO) and has adequate component of officers for analysis of alerts generated by the Anti Money Laundering (AML) system (AMLOCK) procured by the Bank. The Compliance Cell will be analyzing the alerts on transactions handled across

the Bank with the help of system. Also the arrangement is in place to monitor transactions and generate reports on manual basis..

For carrying out the task of analyzing Suspicious Transactions alerts, functionaries at the Compliance Cell will be required to contact Regional Offices as well as branches/offices and their Controllers frequently and repeatedly. All functionaries are required to attend to the request received from the Compliance Cell, over phone, fax, e-mail, or any other established mode of communication, promptly in order to ascertain these alerts as suspicious transaction within the specified time frame. However, the concerned functionaries should not tip off the customer and/or divulge the information called for by the Cell to the customer concerned / others, nor should the transactions in account being investigated should be stopped/restrained. It is reiterated that the communications/investigations are of strictly confidential nature and are required to be handled discreetly. In this connection, it is further clarified that even after establishment of Compliance Cell for system supported monitoring of transactions, Branches/Offices will continue to look for any suspicious transactions/activities at their end and in appropriate cases, arrange to file STRs on the prescribed formats manually to the Compliance Cell, Corporate Office. Also Counterfeit Currency Reports (CCRs) will also be sent as and when any instance of detection of counterfeit currency is observed, to the Compliance Cell at Corporate Office.

9.1 Ongoing Monitoring

The Branches shall exercise ongoing due diligence by carrying out the following activities:

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

(b) To request for or examine the source of funds if it is necessary,

(c) To review and update the document, data, details or information of customers including PEP, high risk customer or of beneficial owner, their business relation, transaction in order to ensure that the same are kept up-to-date,

(d) To regularly monitor cross border correspondent banking and wire transfer and such customers,

(e) To perform other functions as prescribed by the Regulator,

(f) To perform other functions as prescribed by the Bank as deemed necessary from time to time.

10. Reporting Requirements

In terms of rules of the Assets (Money) Laundering Prevention Act, 2008, Compliance Officer is obliged to file following reports to the Financial Information Unit-Nepal Rastra Bank which has been set up as a national unit, for interalia, collecting, analyzing, and disseminating information in respect of financial transactions:

i. Cash /Threshold Transactions Reports (TTRs)
ii. Suspicious Transactions Reports (STRs)

10.1 Transactions of Suspicious Nature

As per the Assets (Money) Laundering Prevention Act, 2008 "Suspicious Transaction" means 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. "Suspicious transaction" means a transaction whether or not made in cash which, to a person acting in good faith:

i. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of Crime or

ii. Appears to be made in circumstances of unusual or unjustified complexity; or

iii. Appears to have no economic rationale or bonafide purpose;

Some of the characteristics to suspect involvement of money laundering activity are as under:

- Involvement of funds in illegal activity
- Intended to hide or disguise assets derived from illegal activities
- Designed to evade anti money laundering guidelines
- No business or apparent lawful purpose

- The sort of transaction in which the particular customer is not normally expected to engage in and for which, after examining available facts, satisfactory linkage is not obtained
- Unusual characteristics or activities
- Attempts to avoid reporting or record keeping requirements
- Provides insufficient or suspicious information

Identifying suspicious activity is to be through transaction history i.e. scrutinizing transactions, which are above the threshold as set in customer profile. Our experiences with the customer in past dealings may also be another source of identification.

Branch officials handling the transactions should use reasonable judgment in determining the suspiciousness of the transaction based on proper monitoring.

It is very important that the customers are neither told nor given any room for doubts in their mind about the course of enquiry while seeking additional information that the Bank is looking at their transactions / activity with suspicion. Such disclosure indication is against the provisions of relevant Act / guidelines.

In case of transactions carried out by a non-account based customer, i.e. a walk-in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. Further, if there is sufficient reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.10 lacs the branch should verify identity and address of the customer and also consider filing a suspicious transaction report in this regard.

Branches are required to record and report all transactions of suspicious nature in deposit, loan accounts and remittances etc., with full details on the prescribed format to the Compliance Officer, Corporate Office, immediately as it has to be immediately reported by Compliance Officer to FIU, NRB.

A copy of the format for reporting, with guidelines for filling up the same is enclosed as Annexure 'C' .Soft copy/updated copy of the format is available on FTP site of the Bank and can be downloaded as and when required. Submission of STR has to be kept confidential and branches are cautioned against tipping off the customers who are being reported upon. The illustrative list of suspicious transactions has been furnished as Annexure 'E'.

Bank has decided to fix following thresholds, subject to review from time to time, for filtering transactions and generating STR alerts.

10.2 Transaction Thresholds for filtering Transactions for STR Purposes

A. Deposit Accounts:

S.N.	Particulars	Low Risk	Medium Risk	High Risk
1.	All deposit accounts pertaining to Governmental bodies/corporations/companies/organizations and JVs with Govt., Regulators, FIs, and Statutory bodies	Rs. 100 lacs	NIL	NIL
2.	All deposit accounts of salaried persons, pensioners, households, students	Rs.10.00 lacs	Rs.8.00 lacs	Rs.5.00 lacs
3.	All deposit accounts of agriculturists, rural artisans, labourers,	Rs.10.00 lacs	Rs.8.00 lacs	Rs.5.00 lacs
4.	Accounts other than individuals and not covered under 1 above.	Rs.25.00 lacs	Rs.15.00 lacs	Rs.10.00 lacs
5.	All non face to face deposit accounts, including NRI accounts,	NIL	NIL	All transactions

B. Advances Accounts

S.N	Particulars	Low Risk	Medium Risk	High Risk
1	Working Capital Loans	FBL or Rs.10.00 lacs whichever is higher	75% FBL or Rs.8.00 lacs whichever is higher	60% FBL or Rs.6.00 lacs whichever is higher
2	Project Loans	Total loan amount or Rs.10.00 lacs whichever is higher	75% of the loan amount or Rs.8.00 lacs whichever is higher	60% of the total loan amount Rs.6.00 lacs whichever is higher
3	Personal Overdraft	OD limit or Rs.10.00 lacs whichever is higher	75% OD limit or Rs.8.00 lacs whichever is higher	60% OD or Rs.6.00 lacs whichever is higher
4	Loan repayable in EMI	Liquidation within one year (from 1st debit closure)	Liquidation within one year (from 1st debit closure)	Liquidation within one year (from 1st debit closure)
5	Loan against FD, NSB, Approved Gov. Bond, etc	Limit or Rs. 10.00 lacs	75% of limit or Rs.8.00 lacs whichever is higher	60% of limit or Rs.6.00 lacs whichever is higher
6	All NPA accounts	N.A.	N.A.	Rs. 5.00 lacs
7	Borrowal accounts pertaining to Governmental bodies/corporations/companies/ organizations and JVs with Govt., Regulators, FIs, and Statutory bodies	Rs. 100 lacs	N.A.	N.A.

11. Combating of Financing of Terrorism

a) In terms of Assets (Money) Laundering (Prohibition) Rules, suspicious transaction should include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Banks have been, therefore, advised to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Information Unit – NRB on priority.

b) As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of Nepal, Nepal Rastra Bank circulates these to all banks and financial institutions. These lists are forwarded to the branches for information and necessary action. Banks/Financial Institutions should ensure to update the consolidated list of individuals and entities as circulated by NRB.

Further, the updated list of such individuals/entities can be accessed in the United Nations website at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml. US Sanction List can be accessed in http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx and UK sanction List http://www.hm-treasury.gov.uk/financialsanctions. Further, order for freezing of assets/fund of sanctioned individual terrorist, terrorist group or terrorist organization can be assessed at the website of Ministry of Home Affairs of Nepal at the link http://www.moha.gov.np/home/pageDetails/72. Branches/Offices are advised that before opening any new account it should be ensured that the name(s) of the proposed customer does not appear in the list. Further, the Branches/Offices should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to Compliance Officer, Corporate Office for inward submission of the same to FIU, NRB.

11.1 Terrorism Finance

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

a. Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts with them.

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

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

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

(ii) Freezing of financial Assets

a. U/s 80.of the BAFIA, Nepal Rastra Bank may request Bank to freeze the accounts or assets held by or for the benefit of the designated individuals/entities. If such request is received from NRB, the Compliance Officer will send freeze order to the concerned branches requesting them to freeze such accounts within 24 hours of receipt of NRB request.

b. The freeze order as aforesaid shall take place without prior notice to the designated individuals/entities.

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

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned Branch. The Branches shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the Compliance Officer, Corporate Office within two working days. The Compliance Officer shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, puts up a note to the Chief Risk and Compliance Officer who then will pass an order within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned branch. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, Compliance Officer shall inform the applicant through the concerned Branch.

(iv) Screening of All Account opening requests before opening account:

Head-MIS will ensure to put in place suitable mechanisms in the system of the Bank that no accounts are allowed to be opened in the name of banned entities and individuals as communicated by NRB from time to time. In case of false name matches the Branch

Manager/Officer-in-charge will be required to white-list such false name matches and permit opening of account under his signatures.

The KYC/MLRO Officer in the Branch should invariably check all account opening requests against above referred lists and must stamp the account with result of such cross check.

12. Maintenance and Preservation of Records

All documents and other information related to the identification and verification of customer and beneficial owner and documents and records related to domestic and foreign transaction with the client and or beneficial owner and records pertaining to account opening must be preserved at least 10 years from the date of cessation of the transaction with the client. The identification records and transaction data should be made available to the competent authorities upon request.

The Bank shall keep the report of suspicious transaction for 10 years.

13. 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.

14. Risk Management

While the Bank has adopted a risk based approach to the implementation of this Policy, it is necessary to establish appropriate framework covering proper management oversight, systems, controls and other related matters.

(i) Bank's Internal Audit will provide an independent evaluation of compliance with KYC/AML Policy including legal and regulatory requirements. Internal Auditors shall specifically check and verify the application of KYC/AML procedures at the Branches/Offices and comment on the lapses observed in this regard. The compliance in this regard will be placed before the

Audit Committee of the Board at quarterly intervals. Further, report of internal audit in regard to compliance will also be made available to Compliance Cell.

(ii) The Compliance Officer will have overall responsibility for maintaining oversight and coordinating with various functionaries in the implementation of KYC/AML/CFT policy. However, primary responsibility of ensuring implementation of KYC/AML/CFT Policy and related guidelines will be vested with the respective Branches/Offices/Business Groups. Suitable checks and balances in this regard will be put in place at the time of introducing new products/procedures as also at the time of review of existing products/procedures for overall risk and compliance management. For this purpose, each Branch/Office/Business Group will designate an official as KYC Compliance Officer/Money Laundering Reporting Officer (MLRO) of the Branch/Office who would ensure proper implementation and reporting, as per provisions of this Policy, to the Compliance Officer.

15. Compliance Officer

The Head- Compliance Cell shall be the Compliance Officer (also termed as Principal Compliance Officer) for KYC/AML/CFT matters who shall be responsible for implementation of and compliance with this policy. His illustrative duties, in this regard, will be as follows:-

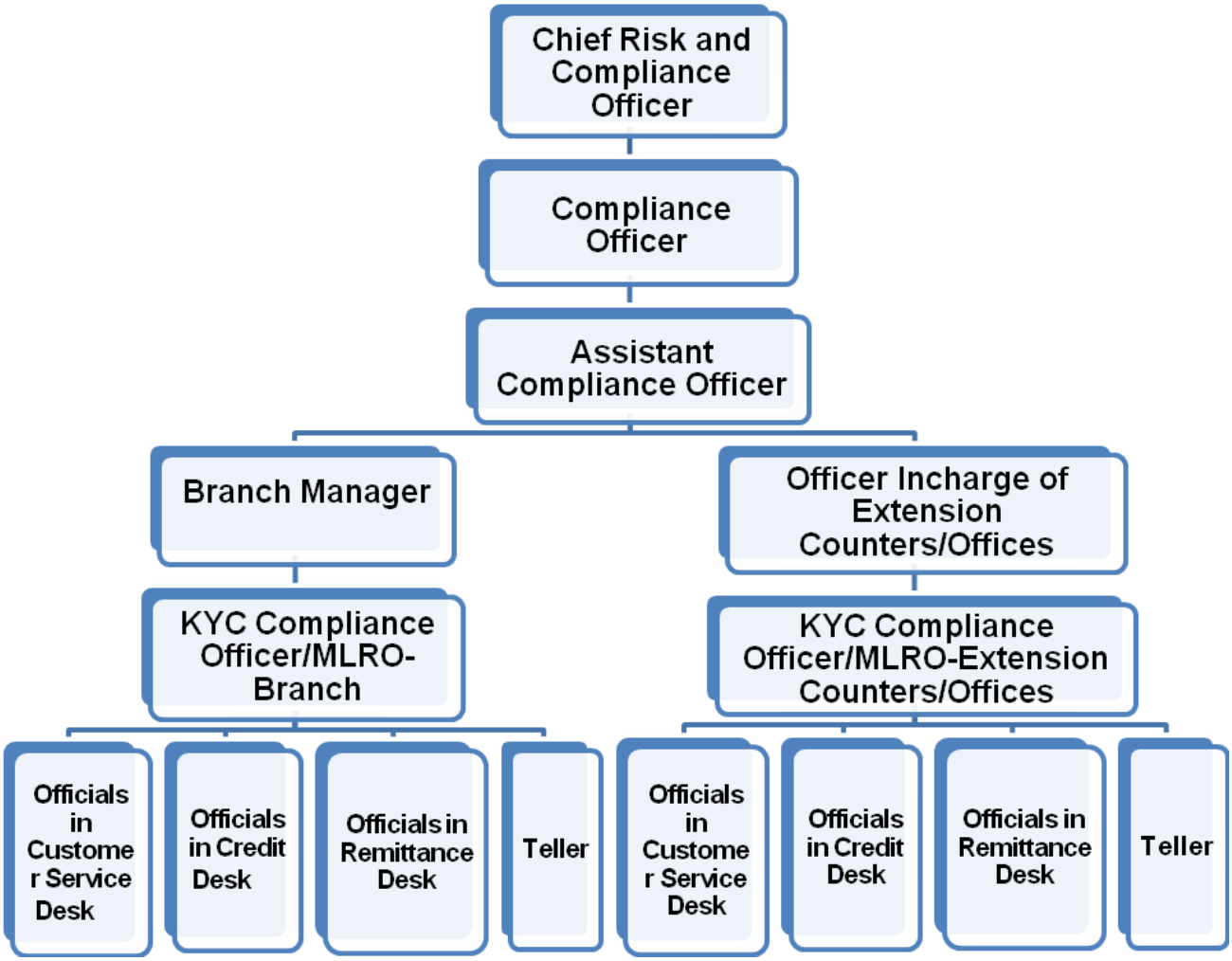
- Overall monitoring of the implementation of the Bank's KYC/AML/CFT policy.
- Monitoring and reporting of transactions, and sharing of information, as required under the law.
- Interaction with MLROs in Branches/Offices/Business Groups for ensuring full compliance with the Policy
- Timely submission of Cash/Threshold Transaction Reports (TTRs) and Suspicious Transaction Reports (STRs) to FIU-NRB
- 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 to the Top Management /Board.
- Performing other KYC compliance related functions as prescribed by FIU-NRB from time to time.
- Updating the list of predicate offenses under the laws and circulating to the Branches/Offices

The Compliance Officer will be supported by necessary number of Officers identified in his/her Cell. These officials will perform their duties, in addition to other roles assigned, as Assistant Compliance Officers as assigned to them by the Compliance Officer.

15.1 To support discharge of responsibilities in an effective manner Officers/In-charges of Customer Service Desk of the Branches/Offices/Business Units have been designated as Money Laundering Reporting Officers (MLROs) and these officials will be responsible for discharge of KYC/AML/CFT related role responsibility in their Branch/Office/Business Unit.

15.2 To facilitate proper monitoring of transactions by Compliance Officer detailed reporting structure has been put in place. In this regard, the Officers working at Compliance Cell and any other officer designated by the HR Department will work as Assistant Compliance Officer(s). The responsibility for reporting TTRs/STRs in respect of transactions held at their respective Branch/Extension counter/Office will lie with the MLRO. They shall report through their respective Branch Manager/Officer In-charge, who in turn, will escalate the matter to the Compliance Officer at Corporate Office, if required.

The flow chart in respect of KYC/AML/CFT reporting will thus look as under:


Chief Risk and Compliance Officer
Compliance Officer
Assistant Compliance Officer
Branch Manager
Officer Incharge of Extension Counters/Offices
KYC Compliance Officer/MLRO-Branch
KYC Compliance Officer/MLRO-Extension Counters/Offices
Officials in Custome r Service Desk
Officials in Credit Desk
Officials in Remittance Desk
Teller
Officials in Custome r Service Desk
Officials in Credit Desk
Officials in Remittance Desk
Teller

16. Reporting system

FIU-NRB entertains reporting only by designated Compliance Officer. Accordingly, all reporting of TTRs and STRs to FIU-NRB will be done only by the Compliance Officer and in his absence by the Assistant Compliance Officer(s).

All the Branches/Offices/Business Units will follow undernoted reporting arrangement.

i. Extraction of TTRs will be centralized at Compliance Cell, Corporate Office through necessary modules developed by MIS Department and reporting to FIU-NRB will be done by the Compliance Officer. Relevant TTRs will be forwarded to MLROs of the Branches/Offices/Business Units every week through email for record and analyzing patterns of transactions to zero on prima facie suspicious transactions, if any.

ii. All transactions will be filtered at MIS Department through core banking system and/or at Compliance Cell, Corporate Office through AMLOCK to generate alerts on prima facie suspicious transactions based on thresholds fixed by the Bank for such filtration. MIS Department, Corporate Office will forward these alerts generated at core banking system to Compliance Cell, Corporate Office for ultimate analysis at relationship point. The Compliance Cell at Corporate Office shall analyze such alters forwarded by MIS Department and generated through AMLOCK under advice to the MLRO of the respective Branch/Office/Business Unit if required and record their comments/observation in respect of all alerts not found suspicious. Alerts which are found prima facie suspicious at the Branches/Offices/Business Units will be forwarded by way of suspicious transaction reports to the Compliance Officer for finalization and reporting to FIU-NRB if found suspicious. While finalizing any STR for the purpose of reporting to FIU-NRB, the Compliance Officer will compulsorily consult Chief Risk and Compliance Officer.

16.1 Scrutiny of unusual transactions that may lead to suspicion should be done by officials at branches/offices on a daily basis as indicated below:

Amount involved –Scrutinizing official

Particulars of Transactions		**Scrutiny By**
Cash transactions upto Rs.1,00,000/-	Transfer transactions upto Rs. 4,00,000/-	Teller/Assistant for transactions handled by him/her
Cash transactions upto Rs.2,00,000/-	Transfer transactions upto Rs. 5,00,000/-	Officer/In-charge-Cash/Remittance for transactions handled by him/her
Cash transactions above Rs.2,00,000/-	Transfer transactions above Rs. 5,00,000/-	Branch Manager/Officer-in-charge
And any transactions not falling under the power of the above mentioned Officials		

16.2 Suspicious Transactions:

To observe “four eyes” concept in reporting suspicious transactions at branch level, first dealing staff at the branch will report to the KYC Officer of the Branch/MLRO who will get himself satisfied about existence of a suspicious activity/nature and then report to the Compliance Officer through the Branch Manager. The Compliance Officer will finalize the decision regarding filing of STR to FIU under advice to Chief Risk and Compliance Officer.

Relevant Information/details regarding submission of STR will also be submitted to the Bank's Board through Risk Management Committee of the Board (RMCB) in its quarterly review.

16.2.1 The BM has to certify in their Monthly **Certificate** that compliance of KYC/AML/CFT guidelines has been done as required.

16.2.2 KYC/AML Inspection & Audit: Internal Audit and the Regional Manager shall carry out audit/inspection of KYC/AML compliance status at the Branches at least once in a year or more frequent intervals and submit Inspection Report to the Chief Operating Officer. Further, report of internal audit/Regional Manager in regard to compliance will also be made available to Compliance Cell. Compliance Cell may also conduct surprise KYC/AML Inspection of the Branches as instructed by the Chief Risk and Compliance Officer with or without notice to the Branches.

16.2.3 Regional Office will submit the particulars of such incidents pertaining to branches under it reported and the action taken in a prescribed format to Internal Audit Department at quarterly intervals for reporting to the Audit Committee of the Board.

16.2.4 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 to any individual/entity having direct/indirect link to banned entities/individuals, as per list of such entities/individuals advised by NRB from time to time and duly circulated by the Bank.

17. Duties and Responsibilities

The chain of duties and responsibilities at branches/Regional Office will be as under:

Personnel Duties	Responsibilities
Employee / officer in charge of customer Service Dept. / officer vested with the authority to open new accounts.	• To interview the potential customer • To verify the introductory reference/customer details / profile. • To exercise due diligence in identifying suspicious transactions. • To ensure against opening of accounts in the names of terrorist/banned organisations. • To comply with the guidelines issued by the Bank from time to time in respect of opening and conduct of account.
Branch Manager	• To scrutinize and satisfy himself/herself that the information furnished in the account opening form / customer profile / are in strict compliance with KYC guidelines before authorizing opening of account. • To certify in the Branch Manager's Monthly Certificate regarding compliance with KYC guidelines and report suspicious transactions to appropriate authority.
Internal Audit	• To verify and record his comments on the effectiveness of measures taken by the branches / level of implementation of KYC guidelines.
Regional Manager	• To ensure prompt reporting of prima facie suspicious transactions to the Compliance Officer. • To verify KYC Compliance at branches during branch visits. • To coordinate with Compliance Officer for conducting trainings on KYC/AML/CFT matters

18. Employee Training

All employee training programmes, of 2 days' duration or more, will have a module on KYC Standards/AML/CFT Measures so that members of the staff are adequately trained in KYC/AML/CFT procedures. Special one day capsule modules will be developed and implemented to provide specialised training in this area to all categories of staff.

Compliance Cell is conducting KYC/AML/CFT trainings/seminars at regular intervals at various Centers as per yearly/quarterly training calendar prepared by the HR Department, so that necessary awareness in regard to Bank's obligations under AMLPA, 2008 as well as NRB/FIU guidelines are disseminated to all levels of Bank's functionaries specially MLROs and Branch Managers who have been vested with the responsibility of ensuring meticulous compliance with KYC/AML/CFT Regulations.

19. Importance of KYC for Employees

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.

Head-HR will ensure that proper Know Your Employee (KYE) Policy and Procedures are put in place, duly circulated and followed strictly to ensure that unwanted individuals do not have access to the Bank by way of employment. He/she will also ensure that any prima facie suspicious activity/behaviour from AML/CFT angle is reported to the Compliance Officer for finalisation and reporting to FIU-NRB wherever required. Bank's KYE Policy and Procedures will be finalized by the Head-HR Department within 6 months from the date this Policy comes into effect.

20. Recruitment/Hiring of Employees

KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse channels of the Bank. Bank will put in place necessary and adequate screening mechanism as an integral part of its recruitment/hiring process of personnel.

21. Customer Education

The Bank recognizes the need to spread awareness on KYC, Anti Money Laundering measures and the rationale behind them amongst the customers and shall take suitable steps for the said purpose. The roles and responsibilities of the customers on KYC/AML measures will be displayed at the Branches/Offices/Business Units in the form of poster/display boards, etc.

22. Correspondent Banking

This policy will apply to our dealings with correspondent banks. For correspondent banking relationship an appropriate due diligence procedure will be laid down keeping in view KYC standards existing in the country where the correspondent bank is located and the track record of the correspondent bank in the fight against money laundering and terrorist financing. The Bank's Treasury Department, Corporate office shall conduct CDD for the Bank's existing correspondent banks within 3 months from **the end of each fiscal year.**

23. Miscellaneous

- Information collected from the customers for KYC compliance should be relevant to the perceived risk, not intrusive and should be treated as confidential. The same is not to be used/divulged for cross selling or any other such purpose.
- Any remittance of funds by way of demand drafts, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value Rs.50,000 and above is effected only by debit to customer's account or against cheques/drafts and not against cash.
- Of late, it has been observed that monitoring of accounts of Non-Profit Organisations, Non-Governmental Organisations, Trusts and fiduciary agencies are posing a challenge to Banks in respect of KYC/AML compliance as such agencies have a mix of complex structure, range of activities, number of persons involved, sources of funds, beneficiaries of funds and types of activities supported by such entities. Branches are therefore, specifically advised to monitor transactions in such accounts with more than ordinary care and in case any suspicious activities/ transactions is detected, the respective MLROs should forward the same to the Compliance Officer through their Branch Managers for finalization.
- Branches should also note that suspicious activity reports are required to be filed even in respect of abandoned transactions, unscrupulous enquiries by individuals and forfeiture of activities / transactions after enquiries are made.
- Such suspicious activity reports should be prepared by respective MLRO and routed through the respective Branch Manager.

24. Review of the Policy

This Policy will be reviewed at least once in a year. However, it can be reviewed more frequently as and when considered necessary by the Board.

Annexure: A

Branch shall obtain following information/documents from the customers depending on the type of the customer. Further, where necessary, private interview of the customer shall also be taken.

(A) Relating to customer deposit

(a) Personal Accounts

1. Name and surname
2. Date of Birth
3. Permanent address
4. Temporary/residential Address (Supporting documents are to be submitted. Such documents may be electricity and water bill and location map prepared by bank staff on site visit (if necessary), voter identity Card, land ownership document etc.)
5. Telephone number both land line and mobile number (if available)
6. Copy of Citizenship/passport (number and description)
7. Copy of identity card in case of an employee of the Government of Nepal or of the entity owned by the Government of Nepal.
8. Photo
9. Permanent Account Number (If available)
10. Name of spouse, undivided family members and three generation details
11. Name of father-in-law (in case of married woman)
12. Occupation (with name and address of employer/business, position and estimated annual income)
13. Other required documents (may be specified from time to time)

Note: In case of customer requiring enhanced customer due diligence, copy of citizenship certificate (minor identity card in case of minor) of all members of undivided family

(b) Accounts of Partnership or Proprietorship firm

(1) Name of the firm

(2) Full Address (Registered address and if registered address changed, also changed address)

(3) Telephone/mobile number/fax number, email address (if available)

(4) Firm registration certificate and PAN Registration Certificate

(5) Details of proprietor, partners and account operators (Position, name, surname, name of spouse, three generation details, permanent address, residential/current address, telephone number, mobile number, email address)

(6) Photos and copy of citizenship certificate or National ID Card of proprietor, partners and account operators

(7) Partnership Deed in case of partnership firm

(8) In case of partnership firm, authorization letter regarding operation of financial and administrative transaction.

(9) Nature of Business and Working area

(10) Number of Branches/Offices and location of major branches/offices

(11) Expected Annual Turnover

(12) In case of firm requiring to be audited, audited financial statements of last fiscal year (if the firm is not required to be audited, self declaration of proprietor/partner in this regard)

(13) Other required documents (may be specified from time to time)

(c) Accounts of Companies

(1) Name of company

(2) Full Address (Registered address and if registered address changed, also changed address) and address of Head Office

(3) Telephone Number, fax number, email address, website (if available)

(4) Certificate of incorporation, Operating license, PAN registration certificate, Memorandum of Association and Article of Association (In case of the organized institutions incorporated under Special Act, documents related to incorporation will not be mandatory)

(5) Details of all members of Board of Directors, Chief Executive Officer and account operators (Position, name, surname, name of spouse, three generation details, permanent address, residential/current address, telephone number, mobile number, email address)

(6) Photos and copy of citizenship certificate or National ID Card of all members of the Board of Directors, Chief Executive Officer and account operators.

(7) Board resolution and authorization for opening of account and operation of account

(8) Authorization by Board of directors to Chief Executive Officer or other officer for conducting financial transactions.

(9) Nature of Business and Working Area

(10) Number of Branches/Offices and location of major branches/offices

(11) Expected Annual Turnover

(12) Audited Financial Statements of Last Fiscal Year

(13) Name and address of parent company if the company is subsidiary of foreign company,

(14) Other required documents (may be specified from time to time)

(d) Accounts of Club/Non-governmental Organization

(1) Name of Club and Non-governmental Organization

(2) Full Address (Registered address and if registered address changed, also changed address)

(3) Telephone Number, fax number, email address, website (if available)

(4) Certification of registration and PAN registration certificate

(5) Constitution of the Organization or clubs.

(6) Details of members of Executive committee, Chief Executive Officer and account operators (Position, name, surname, name of spouse, three generation details, permanent address, residential/current address, telephone number, mobile number, email address)

(7) Photos and copy of citizenship certificate or National ID Card of all members of executive committee, chief executive officer and account operators of club and Nongovernmental Organization

(8) Executive committee's decision and authorization for opening of account and operation of account

(9) Authorization for operation of accounts and financial transactions.

(10) Nature of Business and Working area

(11) Number of Branches/Offices and location of major branches/offices

(12) Expected Annual Turnover

(13) Audited Financial Statements of Last Fiscal Year

(14) Other required documents (may be specified from time to time)

(e) Account of Cooperatives

(1) Name of Institution

(2) Full Address (Registered address and if registered address changed, also changed address)

(3) Phone No., fax no, email address, website (if available)

(4) Certificate of Registration and PAN registration certificate

(5) Constitution

(6) Details of Board of Directors, Chief Executive Officer and account operators (Position, name, surname, name of spouse, three generation details, permanent address, residential/current address, telephone number, mobile number, email address)

(7) Photos and copy of citizenship certificate or National ID Card of Board of Directors, Chief Executive Officer and account operators

(8) Board's resolution regarding opening of account and authorization to conduct financial transactions.

(9) Nature of Business and working area

(10) Number of Branches/Offices and location of major branches/offices

(11) Expected Annual Turnover

(12) Audited Financial Statements of Last Fiscal Year

(13) Other required documents (may be specified from time to time)

(f) Accounts of Public and Private Trust (Guthi)

1. Name
2. Full Address (Registered address and if registered address changed, also changed address)
3. Phone No., fax no, email address, website (if available)
4. Certificate of Registration and PAN registration certificate
5. Constitution of the trust
6. Agreement relating to the establishment of the Trust.

7. Details of directors or members of management committee, Chief Executive Officer and account operators (Position, name, surname, name of spouse, three generation details, permanent address, residential/current address, telephone number, mobile number, email address)

8. Photos and copy of citizenship or National ID Card of directors or members of management committee, Chief Executive Officer and account operators

9. Resolution of Board/Management committee regarding opening of account and authorization to conduct financial transactions.

10. Nature of Business and working area

11. Number of Branches/Offices and location of major branches/offices

12. Expected Annual Turnover

13. Audited Financial Statements of Last Fiscal Year

14. Other required documents (may be specified from time to time)

(g) Accounts of School, Campus or other educational entity

(1) Name of School or Campus

(2) Full Address (Registered address and if registered address changed, also changed address)

(3) Phone No., fax no, email address, website (if available)

(4) Certificate of Registration, PAN registration certificate

(5) Constitution or Memorandum of Association and Article of Association

(6) Certificate of Approval

(7) Details of directors or members of management committee, Chief Executive Officer and account operators (Position, name, surname, name of spouse, three generation details, permanent address, residential/current address, telephone number, mobile number, email address)

(8) Photos and copy of citizenship or National ID Card of directors or members of management committee, Chief Executive Officer and account operators

(9) Resolution of Board/Management committee regarding opening of account and authorization to conduct financial transactions.

(10) Nature of Business and working area

(11) Number of Branches/Offices and location of major branches/offices

(12) Expected Annual Turnover

(13) Audited Financial Statements of Last Fiscal Year

(14) Other required documents (may be specified from time to time)

(h) Accounts of International Non-governmental Organization

(1) Name of Organization

(2) Full Address (Registered address and if registered address changed, also changed address)

(3) Phone No., fax no, email address, website (if available)

(4) Certificate of Registration and PAN registration certificate

(5) Copy of agreement with Social Welfare Council, if any

(6) Copy of agreement with Nepal Government, if any

(7) Charter of the organization

(8) Recommendation letter of concerned country or embassy of the concerned country (In case of International Non-governmental organizations other than licensed or affiliated by authorized body of Nepal)

(9) Details of directors, Chief Executive Officer, representative or chief appointed for Nepal and account operators (Position, name, surname, name of spouse, three generation details, permanent address, residential/current address, telephone number, mobile number, email address)

(10) Photos and copy of citizenship or National ID Card or passport of directors, Chief Executive Officer, representative or chief appointed for Nepal and account operators

(11) Organization's authorization to open account and authorization for financial transactions.

(12) Nature of Business and working area

(13) Number of Branches/Offices and location of major branches/offices

(14) Expected Annual Turnover

(15) Audited Financial Statements of Last Fiscal Year

(16) Other required documents (may be specified from time to time)

(i) Account of Foreign Individual

(1) Full Name

(2) Address in Foreign country (Permanent and temporary)

(3) Address and contact place in Nepal

(4) Name of spouse and three generation details

(5) Copy of the valid visa

(6) Copy of passport

(7) Recommendation letter of the employer organization (in case of employee)

(8) Other required documents (may be specified from time to time)

(j) Accounts of Foreign Company

(1) Name of company

(2) Address of head office of the foreign company in foreign country

(3) Address of the company in Nepal

(4) Nature of office in Nepal (Branch, contact office, project or other)

(5) Certificate of registration in foreign country

(6) Documents relating to incorporation of the foreign company

(7) Information/documents relating to registration of company in Nepal (if any)

(8) Memorandum of Association and Articles of Association of the company.

(9) Authorization provided by foreign *(parent)* company for opening of account and conducting financial transaction

(10) Details of directors and Chief Executive Officer of foreign company (Position, Name, Surname, Address, Telephone number, Mobile number, Email Address)

(11) Details of representative appointed for Nepal and account operators (Position, name, surname, name of spouse, three generation details, permanent address, residential/current address, telephone number, mobile number, email address)

(12) Photos, copy of citizenship certificate or national ID card or passport and document confirming address of two principal executives of foreign company, representative appointed for Nepal and account operators

(13) Business permit issued by the Government of Nepal

(14) Nature of Business and working area

(15) Number of Branches/Offices and location of major branches/offices

(16) Expected Annual Turnover

(17) Audited Financial Statements of Last Fiscal Year

(18) Other required documents (may be specified from time to time)

(k) Accounts of Diplomatic Mission/Embassy

1. Letter of Mission/Embassy
2. Authorization for operation of the account
3. Full Name, address, photo of the account operator and documents confirming the address.
4. Other required documents (may be specified from time to time)

(l) Accounts of Non-Resident Nepalese.

1. Name, surname and address.
2. Name of spouse and three generation Details
3. Documents disclosing source of income
4. Copy of ID of Non-resident Nepalese issued by authorized body of Nepal Government
5. Agreement with employer organization/Appointment letter (if any).
6. Certified copy of passport
7. Full Address and contact place in Nepal.
8. Other required documents (may be specified from time to time)

(B) Customer with no account in the concerned bank

With respect to the customers requesting remittance to other place and customers requesting payment of remittance, branch shall identify such customer appropriately and maintain the records of name and addresses of such customers safely so as to be able to retrieve at the time of need. Further branch shall obtain Citizenship/National ID card/ Photo ID card and documents establishing the temporary address and contact no.

Annexure B

Introduction Requirements and Eligible Introducer

It is essential that any one of the persons from amongst the list of eligible introducers prescribed under should introduce the prospective customer. It is preferable that introducer should come to bank for introduction. However, in case it is not possible for the introducer to come to the bank, it is very important that signature of the introducer should be verified with utmost care and if possible the introduction may be confirmed with the introducer on telephone/ in writing. In case of telephonic confirmation, BM shall record the same in the introduction area of the A/c opening form. A copy of any document establishing identity/residential location of the introducer (who is not a customer of the Bank) is a must. However, depending on the situation and in exceptional cases, the branches/ extension counters may open account without getting any introduction from any such eligible introducer, which will be judiciously exercised by the BM/ Officer in – charge. Reason for doing so should be clearly recorded by the concerned official so also his/her satisfaction regarding credentials of such persons.

List of Eligible Introducers:

The introduction may be obtained from any one of the following persons:

- Existing account holder of the Bank.
- Gazetted officer of the Government of Nepal or Government Agencies (Army officer, Police officer, NRB officer, government school teachers, Officer of any government owned entities, etc.)
- Notary Public
- Professional organizations such as FNCCI, Nepal Medical Association, Nepal Bar Association, ICAN etc.
- Employer company, firm or organization of the applicant(if the branch is satisfied)
- Public or Private School/College/University in which the applicant is a student(if the branch is satisfied)

Annexure C

I. Suspicious Transaction Reports (STR) Form for Branch/Extension Counter

A. Reporting Branch/Officer/Extension Counter:	
1.Name of the Branch/Officer/Extension Counter:	
B. Details of the Customer:	
1.Name of the account holder/s/ customer:	
2. Address:	
3.Profession(if applicable):	
4.Nationality(if applicable):	
5.Other account(s) number (if any):	
6.Other business (if any):	
7.Father/Mother's name (if applicable):	
8.Date of birth/establishment:	
C. Account/Transaction Details	
1.Account Number/Transaction:	
2.Nature of account/transaction:	
(Current/saving/loan/ remittance other pls specify)	
3.Nature of ownership:	
(Individual/proprietorship/partnership/company/other, pls specify)	
4.Date of opening/transaction:	
5.Other account(s) number/transaction (if any):	
6.Amount:	
7.Others:	
(Cash/Transfer/Clearing/TT etc.)	

D. reason for considering the transaction(s) as unusual/suspicious?	
a. Identity of clients	
b. Activity in account	
c. Background of client	
d. Multiple accounts	
e. Nature of transaction	
f. Value of transaction	
g. Other reason (Pls Specify)	
E. Suspicious Activity Information	

Summary Characterization of suspicious activity:

a. Corruption/Gratuity	e. False Statement	i. Structuring
b. Cheque fraud	f. E or wire frauds (debit/credit or other card)	j. Mysterious Disappearance/behaviour
c. Tax evasion	g. Identity theft	k. Counterfeit instrument
d. Loan fraud	h. Terrorist Financing	l. Misuse of position or self
m. Other as mentioned under Point D		

F. Has the suspicious transaction/activity had a material impact on or otherwise affected the financial soundness of the bank/if

Yes ☐ No ☐

Authorized Signature

Name:

Designation: Compliance Officer

Phone:

Fax:

Email:

Date:

II. Suspicious Transaction Reports (STR) Form for Branch/Extension Counter

Name of the Reporting Branch/Office/Extension Counter:							
S.N.	**Name and Address of the person holding account(Including Legal)**	**Branch**	**Date of Transaction**	**Nature of Transaction**	**Amount**	**Reason to be suspicion**	**Remarks**
1							
2							

Authorised Signature
Name:
Designation:
Phone:
Fax:
Email:
Date:

Annexure D

Form for Review of Accounts

Know Your Customer (KYC) and Customer Due Diligence (CDD) Report

Nepal SBI Bank Limited **Know Your Customer (KYC) and Customer Due Diligence (CDD) Report**						
Account Number			Account Title	as per the System		
Customer ID: CTZ or Passport:				as per the Documents		
The Client is Residential	Yes	No		from High Risk Country?	Yes	No
Occupation/Business				Consider High Risk?	Yes	No
List of Documents Obtained:						
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
Proper Residential Address Disclosed					Yes	No
Acceptable Documents submitted by the client to verify residential address?					Yes	No
Power of Attorney/Mandate given? If yes then answer the following:					Yes	No
Have you obtained identification of third party signatory (e.g. Mandatee)					Yes	No
Residential address of third party signatory verified?					Yes	No
Relationship between main account holder and third party signatory established?					Yes	No
What is the relationship between main account holder and third party signatory?					Yes	No
Sources of fund?				Source of fund from High Risk Countries	Yes	No
Anticipated Volume/Frequency of Transaction				Do you consider this as high Risk?	Yes	No
Purpose of Account Opened?				Do you consider this as high Risk?	Yes	No
Who is Beneficial Owner/Nominee?				Do you consider this as high Risk?	Yes	No
Have you verified all documents with the original?					Yes	No
The concerned KYC Officer/Operating Incharge/BM consent to submit the remaining required					Yes	No
Document in case of nun submission						
List of Documents which is not submitted						
1						
2						
3						
4						
5						
6						
Agreed date after which the concerned KYC Officer/BM agreed to close the account in case the pending documents were not submitted by the client: Date:						

As per the points mentioned above please recommend your suggestion to categorize the account as:	**High Risk**	**Medium Risk**	**Low Risk**

If you consider the account is to be considered as High Risk Account:		
Did you post the Account categorization detail in the system?	Yes	No
Have you fully understood the source of the wealth/fund of the customer and are you fully satisfied with the explanation submitted?	Yes	No
If yes, write down the details of the wealth/fund of the client:		
1. Threshold limit: (Maximum Estimated credit into A/c in a year (A)		
2. Actual Credit into A/c during the period of one year (in case of old A/c (B)		
IF difference between A and B is 0 its OK . If B is 20% above A then STR		
1. Sources fund explored:		
2. Second verification of Identification		
3. Verification of address:		
4. Any other important information deemed necessary:		

…… **Staff Designated for Account Opening** Date:	…….. **KYC Compliance Officer/Operation Incharge** Date:	…….. **Approved by the BM/Incharge** Date:

Annexure E

The list of suspicious transactions furnished here is not exclusive and staff members would always be expected to monitor transactions of all types which pass through their desks with fair. However, it may be one that is inconsistent with a client's known business, profession or activity/trade he/she carries on amount of judgment and vigilance over and above the normal precautions they would take for completing transactions. The understanding of customer's identity vis-à-vis his stated norms of dealings, services, etc. would also have a bearing on transactions before they are viewed as suspicious transactions. The key to detect such suspicious transactions is to knowing sufficiently about client to recognize that a transaction/or series of them is unusual. Reasonable grounds to suspect" is determined rather more by reasonable circumstances, including normal business practices and systems than automated system depending on the industry. It may vary from business to business, Customer to Customer, place to place, and system to system.

1. Availing exchange for business trips which is disproportionate to the duration of stay and not befitting the status of the business executive of the company.
2. Cash being tendered for availing foreign exchange by corporate customers.
3. Customers who receive various remittances frequently from centers abroad and make various remittances frequently abroad.
4. Frequent visits to same destinations by a large number of officials who draw disproportionately high amount of exchange.
5. Receipt of international remittances from services irrelevant to customer's business/profession or from destinations in countries which are known for money laundering e.g. tax havens and countries which do not have anti money laundering legislations.
6. Money activities in accounts of customers, which show sudden and disproportionate growth in volumes.
7. Customer or his representative reluctant to give information relating to customer's activities.
8. Customer's account exhibiting large deposits through tender of currency bearing the labels of other banks.
9. A single cash deposit of substantial amount comprising of large component of high/low denomination notes.
10. Unlimited applications/requests for drafts/pay orders against cash.
11. Customers requiring exchange of small denominations of notes for larger denominations and vice versa.
12. Several cash deposits/withdrawals below a specified threshold limit to avoid filing a report. These may be necessary in case of transactions above the threshold level, i.e. initial splitting of transactions.
13. Individual/group that induces or attempts to induce the bank employee/s to avoid filing reports/or any other forms.

14. Depositing small amount of cheques but rare big withdrawals.
15. Request for wire transfers, out of country, financed by multiple banker's cheques (just below threshold limit).
16. Customer receiving wire transfers and converting the balances in monetary instruments favoring third parties.
17. Cancellation of Banker's cheques obtained for large amounts favoring Govt. Depts., under the pretext of cancellation of transaction/contract or request for cancellation of drafts/pay order of large sums obtained from the Bank after a lapse of substantial period of time.
18. A customer or a non-customer receives incoming telegraphic transfers "payable on proper identification" and/or to convert the funds to banker's cheques and mail them to customer or non-customer when
    a. The amount is very large, or just below the specified threshold limit decided by the Bank or legislation.
    b. Funds come from a foreign country
    c. Transactions are repeated.

Employees need to be cautious if they encounter the following situations/ transactions and immediately report to the respective Authority:

a. Identification Documents

- Customer provides doubtful or vague information.
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Customer refuses to produce personal identification documents.
- Customer only submits copies of personal identification documents.
- Customer wants to establish identity using something other than his or her personal identification documents.
- Customer's supporting documentation lacks important details such as a phone number.
- Customer inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.
- Customer presents different identification documents at different times.
- Customer alters the transaction after being asked for identity documents.
- Customer presents different identification documents each time a transaction is conducted.
- Customer provides false information or information that is unreliable.
- Customer spells his or her name differently from one transaction to another.

b. Cash Transactions

- Customer starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the Customer in the past.
- Customer frequently exchanges small bills for large ones.
- Customer uses notes in denominations that are unusual for the Customer, when the norm in that business is different.
- Customer presents notes that are packed or wrapped in a way that is uncommon for the Customer.

- Customer deposits musty or extremely dirty bills.
- Customer makes cash transactions of consistently rounded-off large amounts.
- Customer consistently makes cash transactions that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.
- Customer presents uncounted funds for a transaction. Upon counting, the Customer reduces the transaction to an amount just below that which could trigger reporting requirements.
- Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Customer frequently purchases traveler's cheques, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the Customer.
- Customer asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the Customer.
- shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.)
- Stated occupation of the Customer is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Cash is transported by a cash courier.
- Large transactions using a variety of denominations.

c. Economic Purpose

- Transaction seems to be inconsistent with the Customer's apparent financial standing or usual pattern of activities.
- Transaction appears to be out of the normal course for industry practice or does not appear to be economically viable for the Customer.
- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- A business Customer refuses to provide information to qualify for a business discount.
- No business explanation for size of transactions or cash volumes.
- Transactions of financial connections between businesses that are not usually connected (for example, a food importer dealing with an automobile parts exporter).
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

d. Identification Address

- Customer does not want correspondence sent to home address.
- Customer repeatedly uses an address but frequently changes the names involved.
- Customer's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact Customer shortly after opening account.
- Normal attempts to verify the background of a new or prospective Customer are difficult.
- Customer uses aliases and a variety of similar but different addresses.
- Customer hesitates to provide his easy address and contact.

e. Physical Background and Personal Behaviours

- Customer is nervous, not in keeping with the transaction.
- Customer has only vague knowledge of the amount of a deposit.
- Customer presents confusing details about the transaction or knows few details about its purpose.
- Customer appears to informally record large volume transactions using unconventional bookkeeping methods or "off-the-record" books.
- Customer appears to be acting on behalf of a third party, but does not tell you.

- Customer is involved in activity out-of-keeping for that individual or business.
- Customer insists that a transaction be done quickly.
- Inconsistencies appear in the Customer's presentation of the transaction.
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the Customer.
- Customer attempts to develop close rapport with staff.
- Customer pays for services or products using financial instruments, such as money orders or traveler's cheques, without relevant entries on the face of the instrument or with unusual symbols, stamps or notes.

f. Criminal Background

- Customer admits or makes statements about involvement in criminal activities
- Customer is accompanied and watched.
- Customer is nervous, not in keeping with the transaction.
- Customer over justifies or explains the transaction.
- Customer is secretive and reluctant to meet in person.
- Information that a Customer is the subject of a money laundering or terrorist financing investigation.
- Information that a Customer is suspected of being involved in illegal activity.
- A new or prospective Customer is known to you as having a questionable legal reputation or criminal background.
- Customer offers money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious.
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).

g. Transactions Involving Accounts

- Customer appears to have accounts with several financial institutions in one area for no apparent reason.
- Customer conducts transactions at different physical locations in an apparent attempt to avoid detection.
- Opening accounts when the Customer's address is outside the local service area.
- Opening accounts in other people's names.
- Opening accounts with names very close to other established business entities.
- Attempting to open or operating accounts under a false name.
- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Funds are being deposited into several accounts, consolidated into one and transferred outside the country.
- Customer frequently uses many deposit locations outside of the home branch location.
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.
- Activity far exceeds activity projected at the time of opening of the account.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Account that was reactivated from inactive or dormant status suddenly sees significant activity.
- Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.
- Unexplained transfers between the Customer's products and accounts.
- Large transfers from one account to other accounts that appear to be pooling money from different sources.
- Multiple deposits are made to a Customer's account by third parties.
- Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.
- Frequent deposits of bearer instruments in amounts just below the threshold.

- Unusually large cash deposits by a Customer with personal or business links to an area associated with drug trafficking.
- Regular return of cheques for insufficient funds
- Correspondent accounts being used as "pass-through" points from foreign jurisdictions with subsequent outgoing funds to another foreign jurisdiction.
- Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are in locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Customer appears to have recently established a series of new relationships with different financial entities.

h. Extra-territorial Transactions

- Customer and other parties to the transaction have no apparent ties to Nepal.
- Transaction crosses many international lines.
- Use of a credit card issued by a foreign bank that does not operate in Nepal by a Customer that does not live and work in the country of issue.
- Cash volumes and international remittances in excess of average income.
- Excessive demand for migrant remittances from individuals or entities based on migrant worker population.
- Transactions involving high-volume international transfers to third party accounts in countries that are not usual remittance corridors.
- Transaction involves a country known for highly secretive banking and corporate law.
- Transactions involving any countries deemed by the Financial Action Task Force as requiring enhanced surveillance.
- Foreign currency exchanges that are associated with subsequent wire transfers to locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Deposits followed within a short time by wire transfer of funds to or through locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money-laundering system.
- Transaction involves a country known or suspected to facilitate money laundering activities.

i. Transactions Related to Offshore Business Activity

- Accumulation of large balances, inconsistent with the known turnover of the Customer's business, and subsequent transfers to overseas account(s).
- Frequent requests for traveler's cheques, foreign currency drafts or other negotiable instruments.
- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-dollar deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore "shell" bank whose name may be very similar to the name of a major legitimate institution.
- Unexplained electronic funds transfer by Customer on an in-and-out basis.
- Use of letter-of-credit and other method of trade financing to move money between countries when such trade is inconsistent with the Customer's business.
- Use of a credit card issued by an offshore bank.

j. Miscellaneous

- Customer attempts to convince employee not to complete any documentation required for the transaction.
- Customer makes inquiries that would indicate a desire to avoid reporting.
- Customer has unusual knowledge of the law in relation to suspicious transaction reporting.
- Customer seems very conversant with money laundering or terrorist activity financing issues.

- Customer is quick to volunteer that funds are “clean” or “not being laundered.”
- Customer appears to be structuring amounts to avoid record keeping, Customer identification or reporting thresholds.
- Customer appears to be collaborating with others to avoid record keeping, Customer identification or reporting thresholds.
- Customer performs two or more cash transactions within 24 hours where each transaction is just below the threshold.
- Customer shows uncommon curiosity about internal systems, controls and policies.

Annexure F

General Information and Questionnaire for Correspondent Banking

PART I : Ownership Structure/General Information		
1	Name of Institution:	
2	Date & Place of Incorporation, registered address:	
	Contact No:	
3	License and Certificate of Registration (please provide certified a copy)	
4	Website:	
5	Is your institution publicly owned?	
6	Is your institution listed in any stock exchange?	
7	Name and Website of your regulatory bodies in which you are under supervision:	
	Name:	
	Website:	
8	Money Laundering reporting officer (AMLRO) details:	
	Name:	
	Contact No.	
	Fax:	
	Email:	
9	Compliance Manager details:	
	Name:	
	Contact No.:	
	Fax:	
	Email:	
10	Nature of Business:	
11	Number of Branches:	

PART II: Management and Composition of Shareholders:

1. Please provide a current list of your board of directors and confirm if there is any change in the senior Management level of your institution for the past six months.

a) List of Central Management Committee:

S. No.	Name	Designation	Place of Birth

b) List of Board of Directors:

S. No.	Name	Designation	Place of Birth

2. Please provide us the names of any shareholder who holds 5% percentage or more stakes of your institution (if all are below 5%, please name the top two shareholders). Please provide the ultimate beneficial owner of such shareholder who is an individual. Please also provide their main activities.

Please reply to us to the attention of Treasury Department by authenticated Swift Message or by mail to the following address.

Address: Nepal SBI Bank Ltd.
Forex and Treasury Department
Corporate Office
Kesharmahal, Kathmandu
Tel:
Fax:
E-mail:

PART III. QUESTIONNAIRE:

1. GENERAL AML POLICIES, PRACTICES AND PROCEDURES: (ANSWER YES/NO)	YES	NO
Has the Country in which you are located established laws designed to prevent money laundering?		
Has your institution developed written policies documenting the processes that they have in place to prevents, detect and report suspicious transactions' that has been approved by senior management/ board of Financial Institution		
In addition to inspections by the government supervisors/regulators, does the Financial Institution client have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?		
Does the Financial Institution have a legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML framework?		
Does the Financial Institution have a policy prohibiting accounts/relationships with shell banks? (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.)		
Does the Financial Institution have record retention procedures that comply with applicable law? If yes how long?		
Has your institution been subject to any investigation, indictment, conviction or civil enforcement action related to money laundering and terrorism financing in the past five years.		
Does your country adhere to the 40 anti-money laundering recommendations and 9 special terrorist financing recommendations developed by the Financial Action Task Force (FATF)?		
Does the Financial Institution's AML policies and practices being applied to all branches and subsidiaries of the Financial Institution both in the home country and in locations outside of that jurisdiction?		
2. RISK ASSESSMENT		
Does the Financial Institution have a risk-based assessment of its customer base and their transactions?		
Does the Financial Institution determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the Financial Institution has reason to believe pose a heightened risk of illicit activities at or through the Financial Institution?		

3. KNOW YOUR CUSTOMER, DUE DILIGENCE AND ENHANCED DUE DILIGENCE		
Has your institution implemented systems for identification of its clients, including client information in case of recorded transactions, account opening such as family name/ name of the firm, activities/ job, nationality , street address, tel. Number, country/ state that issued it		
Does your institution have procedures to establish a record for each client noting their respective identification documents and know your client information collected at account opening? Are copies of identification documents retaining in your possession for reference?		
Does the financial Institution collect information and access its Customer"s as per its AML Policies or practices?		
Does the Financial Intuition have policies covering relationships with Politically Exposed Persons (PEP's), their family and close associates?		
Does your institution take steps to understand the normal and expected transactions of its customers based on its risk assessment of its customers based on its risk assessment of its customers?		
Does the Financial Institution have procedures to establish a record for each new customer noting their respective identification documents and 'Know Your Customer' information?		
Does the Financial Institution have process to review and, where appropriate, update customer information relating to high risk client information?		
4. REPORTABLE TRANSACTIONS AND PREVENTION AND DETECTION OF TRANSACTIONS WITH ILLEGALLY OBTAINED FUNDS.		
Does your institution have policies for the identification and reporting of transactions that are required to be reported to the authorities		
Does your institution screen transactions for clients or transactions the financial institutions deems to be of significantly high risk that special attention to such customer or transactions is necessary prior to completing any such transaction?		
Does your institution have procedures to identify transaction structured to avoid large cash reporting requirements?		
Does your institution have policies to reasonably ensure that they will not operate with or on behalf of shell bank throughout any of its account?		
5. TRANSACTION MONITORING		
Does the financial Institutions have a monitoring program for suspicious or unusual activity that covers funds transfers and monetary instruments (such as travelers checks, money orders, etc)?		

6. AML TRAINING		
Does your institution provide AML training to relevant employees that include identification and reporting of transactions that must be reported to govt. authorities, examples of different forms of money laundering involving the bank products and services and internal policies to prevent money laundering?		
Does the FI retain records of its training sessions including attendance records and relevant training material used?		
Does your institution communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?		
Does your institution have an established audit and compliance review function to test the adequacy of AML and terrorist financing procedures?		
Does the Financial Institution employ agents to carry out some of the functions of the Financial Institution and if so does the Financial Institution provide AML training to relevant agents that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving the Financial Institution's products and services and internal policies to prevent money laundering?		
7. DOCUMENTS TO BE WITH ANSWER		
Internal AML Guidelines/Policies :		
Latest Annual Report/Financial Statement :		

……

(signatures)

Name of Compliance Officer : ……

Name of the Bank/ FI / Organization : ……

Address : ……

Tel : ……

Fax :.....

E-mail : ……

Annexure G

List of Predicate Offences

1. **Any offence under the prevailing laws**

a. Participation in an organized criminal group and racketeering,	(क) सङ्गठित अपराधिक समूह र गैरकानूनी वा धुर्त्याइपूर्वकको असूली (र्‍याकेटरिङ्ग) मा सहभागी हुने सम्बन्धी,
b. Disruptive (terrorist) act and terrorism,	(ख) विध्वंसात्मक कार्य लगायत आतङ्कवाद सम्बन्धी,
c. Trafficking in human being and migrant smuggling in any form,	(ग) जुनसुकै प्रकारको मानव बेचबिखन तथा ओसारपसार सम्बन्धी,
d. Any kinds of sexual exploitation including the children,	(घ) बाल यौन शोषण लगायत जुनसुकै प्रकारको यौन शोषण सम्बन्धी,
e. Illicit trafficking in narcotic drugs and psychotropic substances,	(ङ) लागू औषध तथा मनोद्विपक पदार्थको गैरकानूनी ओसारपसार सम्बन्धी,
f. Illicit trafficking in arms and ammunition,	(च) हातहतियार खरखजानाको गैरकानूनी ओसारपसार सम्बन्धी,
g. Illicit trafficking in stolen and other goods,	(छ) चोरी गरिएको वा अन्य वस्तुको गैरकानूनी ओसारपसार सम्बन्धी,
h. Corruption and bribery,	(ज) भ्रष्टाचार तथा घुस सम्बन्धी,
i. Fraud,	(झ) ठगी सम्बन्धी,
j. Forgery	(ञ) कीर्ते सम्बन्धी,
k. Counterfeiting of coin and currency,	(ट) खोटा सिक्का वा मुद्रा सम्बन्धी,
l. Counterfeiting and piracy of products, or imitation, illegal copy or theft of products,	(ठ) नक्कली वस्तुको उत्पादन तथा उत्पादनको गैरकानूनी प्रतिलिपि वा चोरी (पाइरेसी अफ प्रोडक्टस्) सम्बन्धी,
m. Environmental crime,	(ड) वातावरण सम्बन्धी,

n. Murder, grievous bodily injury,	(ढ) ज्यान लिने तथा अङ्गभङ्ग सम्बन्धी,
o. Kidnapping, illegal restraint or hostage-taking,	(ण) अपहरण, गैरकानूनी थुना वा शरीर बन्धक सम्बन्धी,
p. Theft or rubbery,	(त) चोरी वा डकैती सम्बन्धी,
q. Smuggling (including custom, excise and revenue),	(थ) तस्करी (भन्सार, अन्तशुल्क तथा कर सहित) सम्बन्धी,
r. Tax (including direct and indirect),	(द) कर (प्रत्यक्ष वा अप्रत्यक्ष समेत) सम्बन्धी,
s. Extortion,	(ध) आपराधिक लाभ (एक्स्टर्सन) सम्बन्धी,
t. Piracy,	(न) सामुद्रिक डकैती (पाइरेसी) सम्बन्धी,
u. Insider Dealing and Market Manipulation in securities and commodities ,	(प) धितोपत्र वा कमोडिटिज बजारलाई प्रतिकूल प्रभाव पार्ने (मार्केट म्यानिपुलेसन) वा भित्री कारोबार(इन्साइडर ट्रेडिङ्ग) सम्बन्धी,
v. Ancient monument conservation,	(फ) प्राचीन स्मारक संरक्षण सम्बन्धी,
w. Forest, National park and wild animals,	(ब) वन, राष्ट्रिय निकुञ्ज तथा वन्यजन्तु संरक्षण सम्बन्धी,
x. Money, banking, finance, foreign exchange, negotiable instruments, insurance, cooperatives,	(भ) मुद्रा, बैंकिङ्ग, वित्तीय, विदेशी विनिमेय, विनिमेय अधिकारपत्र, बीमा वा सहकारीसँग सम्बन्धी,
y. Black marketing, consumer protection, competition, supply,	(म) कालोबजार, उपभोक्ता संरक्षण, प्रतिष्पर्धा वा आपूर्ति सम्बन्धी,
z. Election,	(य) निर्वाचन सम्बन्धी,
aa. Communication, broadcasting, advertising,	(र) सञ्चार, प्रशारण, विज्ञापन सम्बन्धी,
bb. Tansportation, education, health, medicine, foreign employment,	(ल) यातायात व्यवसाय, शिक्षा, स्वास्थ्य, औषधी वा वैदेशिक रोजगार ठगी सम्बन्धी,
cc. Firm, partnership, company, association,	(व) फर्म, साझेदारी, कम्पनी वा संघ संस्था सम्बन्धी,

dd. Real estate and property,	(श) घर, जग्गा र सम्पत्ति सम्बन्धी,
ee. Lottery, gambling, donation,	(ष) चिठा, जुवा वा चन्दा सम्बन्धी,
ff. Citizenship, immigration and passport.	(स) नागरिकता, अध्यागमन वा राहदानी सम्बन्धी ।

(2) Offence of terrorist financing :
(3) Any other offence as designated by the Government of Nepal by publishing a notice in the Nepal Gazette,
(4) An offence under a law of a foreign State, in relation to act or omission, which had they occurred in Nepal, would have constituted an offence.