Know Your Customer (KYC) and Anti Money Laundering (AML) /Counter Financing of Terrorism (CFT) Policy

2021

Version 4.0

Siddhartha Bank

Approval sheet

Title of Policy: Know Your Customer (KYC) and Anti Money Laundering (AML)/Counter Financing of Terrorism (CFT) Policy

Initiated by	**Saroj Kafle** Head- Compliance and Corporate Governance	
Reviewed by	**Shailaja Gyawali** Head Integrated Risk	
Reviewed by	**Suresh Maharjan** Head Business Support & PSD	
Supported by	**Sundar Prasad Kadel** Chief Executive Officer	

TABLE OF CONTENTS

1. Background and Commencement

The Bank is at the forefront of NRB's continuous initiatives and efforts in the prevention of the use of the banking system for illicit, laundering and terrorism financing activities.

The Bank demonstrates its full commitment and support to high standards of compliance with the Anti Money Laundering/Combating the Financing of Terrorism (AML/CFT) requirements by establishing robust and comprehensive policy, procedures, processes and system for the prevention and detection of money laundering and terrorism financing activities.

This policy and related procedures are subject to periodic reviews to ensure that it remains robust and complies with the regulatory requirements and the international recommendations.

This document is guided by "Asset (Money) Laundering Prevention Act, 2008 (amendment 2019) ", "Asset (Money) Laundering Prevention Rules, 2016", various regulations and directives issued by Nepal Rastra Bank (NRB) and Financial Information Unit (FIU) from time to time. Also, recommendations issued and changes made from time to time by Financial Action Task Force (FATF), Asia Pacific Group on Money Laundering (APG), Basel Committee on Banking Supervision (BCBS) and other international agencies are taken into consideration to this policy document.

This Policy shall be known as "Know Your Customer and Anti Money Laundering Policy".

2. Definitions

Money Laundering
Money Laundering is the participation in any transaction that attempts to conceal or disguise the nature or origin of funds derived from illegal activities such as, fraud, corruption, tax evasion, organized crime, or terrorism etc.

Terrorism Financing
Terrorism Financing refers to any activity that provides funding or financial support of any kind to the terrorist activities. The funds involved may have been raised from the legitimate sources as well as from the criminal sources.

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

Know Your Customer (KYC)
KYC is the process of identifying the customer and verifying the identity by using reliable and independent document and information. It is regarded as the basic tool for AML/CFT and its main objective is to enable the Bank to know and understand its customers better and help them manage their risks prudently. If the Bank is unable to apply appropriate KYC measures due to non-furnishing of information or non-cooperation by the customer, the Bank has right to consider closing the account or terminating the banking relationship after issuing due notice to the customer explaining the reasons for taking such a decision.

Customer
Customer is any person or entity engaged in a financial transaction or activity with the Bank or someone on whose behalf the financial transaction or activity is being performed.
For the purpose of this policy, a customer is a person or entity, who is attached to the Bank through any one or more of the following events/activities:

- maintains an account and/or has a business relationship with the Bank
- engaged in one or more occasional transaction
- involved in carrying out wire transfers
- on whose behalf the account is maintained (i.e. beneficial owner)
- engaged in any business or transaction in any instance

Financial Action Task Force (FATF)
The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognized as the global anti-money laundering (AML) and Combat financing of terrorism (CFT) standard.

Customer Due Diligence (CDD)
CDD is the process through which the Bank develops an understanding of the customers and the ML/FT risks that they pose to the business. CDD is the cornerstone of the AML/CFT program. It involves gathering and verifying information about a customer's identity, beneficial owners and representatives.

Simplified Customer Due Diligence (SCDD)
Simplified Customer Due Diligence is the lowest level of due diligence that can be completed to the customer. Simplified CDD is the information obtained for all customers to verify the identity of a customer and assess the risk associated with that customer. Simplified Due Diligence will be applied, where the customer is considered to present a low risk of money laundering and terrorist financing.

Enhanced Customer Due Diligence (ECDD)
Enhanced Customer Due Diligence is the additional information collected of the customer to provide a deeper understanding of the customer activity to mitigate associated risk. Enhanced Customer Due Diligence is required where the customer and product/services combination is considered to be of higher risk. A high risk situation is where there is an increased risk for money laundering and terrorist financing through customer profiles and way of utilization of the products and services that are being offered to them.

Financial Information Unit (FIU)
Financial Information Unit (FIU) was established on 21 April 2008 to work against the money laundering and terrorism financing activities. It is a central, national agency, responsible for receiving, processing, analyzing and disseminating financial information and intelligence on suspected money laundering and terrorist financing activities to the Investigation Department, other relevant law enforcement agencies and foreign FIUs.

Asia Pacific Group on Money Laundering (APG)
The APG is an autonomous, voluntary and co-operative international body officially established by formal terms of reference endorsed by 13 founding members in February 1997 at the 4th Asia Pacific money Laundering symposium in Bangkok, Thailand, with the following core functions:

- Assessment of compliance of the APG members with the FATF standards on Money Laundering and Terrorism Financing through mutual evaluation
- Coordination and technical assistance and training to the member states
- Conduct research and analysis to enhance the understanding of the issues related to Money Laundering and Terrorist Financing.
- Contribute to the global AML/CFT policy formulation

Beneficial Owner
The "Beneficial Owner" is the natural person who ultimately owns or controls firm and/or a person on whose behalf the transactions is being conducted, and include person or persons who exercise ultimate effective control over a juridical person.

Shell Bank/Entity
As per the Asset (Money) Laundering and Prevention Act 2008, Shell Banks are the financial institutions or a group of financial institutions that have no physical presence in the country of origin or establishment and/or do not fall under any scope of effective regulation and supervision.
A shell company is an entity that has no active business and usually exists only in name as a vehicle for another company's business operations. In essence, shells are corporations that exist mainly on paper, have no physical presence, employ no one and produce nothing. Although they are legal entities that do have a legitimate function in business operations, shell companies are also utilized by criminals to facilitate fraudulent activities including money laundering.

Tipping Off
Tipping off is giving an idea of or disclosing information to the customer or any other unauthorized person(s) that his/her someone's account is being monitored or considered suspicious. Tipping Off is a punishable offence.

FATCA
"FATCA" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.
Payable-Through accounts
Payable-Through accounts refer to the correspondent accounts that are used directly by the third parties, generally the customer of the respondent bank, to transact business on their own behalf.

Nested Accounts
Nested account occurs when a Bank/FI (third party BFI) gains access of the financial services offered by the correspondent bank by operating through the correspondent account belonging to the another Bank/FI i.e. of a respondent Bank/FI.

Wire Stripping
Wire stripping is the deliberate act of altering or eliminating any material information from wire payments or instructions, thereby making the payment message/instruction difficult to identify the sanctioned entity and restrict payments to and from sanctioned parties or countries.

3. Objectives of the Policy

Primarily this policy is prepared and implemented to prevent the Bank from being used for money laundering and terrorism financing activities. The following are the major objectives of this policy:

- To lay down policy framework to be implemented by the Bank in order to safeguard it against being used, intentionally or unintentionally, by criminal elements for money laundering and financing of terrorism.
- To ensure full compliance by the Bank with all the applicable legal and regulatory requirements pertaining to the Anti Money Laundering and Combating the Financing of Terrorism.
- To provide a broad framework for formulation and implementation of procedural guidelines required for effective AML/CFT & KYC compliance.

4. Scope and Application

This policy is applicable to all branches/offices of the Bank and is to be read in conjunction with related Standard Operating Procedures (SOP) and guidelines issued from time to time.

The contents of the Policy shall be subject to changes/modifications as advised by the regulators and/or the Bank from time to time.

Any provision laid down in this policy will be superseded by existing or future provisions of "Asset (Money) Laundering Prevention Act 2008 (amendment 2019) ", "Asset (Money) Laundering Prevention Rules, 2016", regulations issued by Financial Information Unit (FIU) and directives issued by Nepal Rastra Bank (NRB) from time to time.

The standards set by this policy document will apply to both new and existing business relationships and across all the branches/units of the Bank. Hence, in regards to the existing business relationships as well, it is essential to initiate corrective action and customer due diligence, where necessary.

5. Compliance of KYC and AML/CFT Policy

Bank shall ensure compliance with KYC and AML/CFT Policy through:

a. Bank shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.
b. All HO Divisions to ensure compliance of KYC guidelines in their respective areas of operation, products, services, activities etc.
c. Independent evaluation of the compliance functions of Banks policies and procedures, including legal and regulatory requirements to be done by Compliance Division, HO
d. Internal audit system to verify the compliance with KYC & AML/CFT policies and procedures and submit quarterly audit notes and compliance to the Audit Committee. At the end of every calendar quarter, implementation and compliance of concurrent audit reports on adherence to KYC and AML/CFT guidelines at branches would be reviewed for apprising Audit Committee of Board.
e. Concurrent / internal audit to also ensure verification of compliance with KYC guidelines in system through system generated reports from MIS / CBS.
f. The implementation of KYC and AML/CFT policies and guidelines by branches in letter and spirit has to be ensured by the OO/BM/DH and their respective reporting supervisors at Branch Coordination Cell.

6. Money Laundering and Terrorism & Proliferation Financing

6.1 Money Laundering

Money Laundering is the process used to disguise the source of money or assets derived from criminal activity. Money laundering facilitates corruption and can destabilize the economies of susceptible countries. It also comprises the integrity of legitimate financial systems and institutions, and gives organized crime the funds it needs to conduct further criminal activities. Generally, money launderers tend to seek out areas in which there is low risk of detection due to weak or ineffective Anti Money Laundering program. Because the objective of Money Laundering is to get the illegal funds back to the individual who generated them. Therefore, Banks have been the targets for Money Laundering.

While the techniques for laundering funds vary considerably and are often highly intricate, there are generally three stages in the process:

Stages / Process of Money Laundering

Placement: Involves placing the proceeds of crime in the financial system. It refers to the physical disposal of cash, often in the form of bank deposit, through a succession of small and anonymous transactions. The money launderers insert the illicit money into a legitimate financial institution.

Layering: This stage involves converting the proceeds of crime into another form and creating complex nature of financial transactions to disguise the audit trails and the source and the ownership of funds (e.g. buying and selling of commodities, stocks, property etc.). It involves bank to bank transfers, wire transfers, several deposits and withdrawals, purchasing high value items etc.

Integration: In this stage the money re-enters the mainstream economy in the legitimate looking form. It involves placing the laundered proceeds back in the economy under the veil of legitimacy. It would be very difficult to trace the original source of the money if there is no proper documentation in the previous two stages of Money Laundering.

6.2 Terrorism Financing

The financing of terrorism is where funds or other property is made available, directly or indirectly, with the sole intention that the funds be used to further terrorism or to initiate terrorist acts to be carried out. The primary goal of individuals and entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity.
The major source of terrorist financing include financial support from countries, organizations or individuals that may include criminal activities and revenue generating activities, may involve drug trafficking, human smuggling, theft, robbery and fraud to generate money. Funds raised to finance terrorism usually have to be laundered and thus anti-money laundering

processes in the banks and other reporting industries are important in the identification and tracking of terrorist financing activities.
The Bank shall monitor, identify and report funds received or sent for terrorist financing using the bank's system. The Bank shall take caution while doing transaction, account opening or carrying banking activities if in any circumstances the name of any banned or sanctioned organization or individual (involved in terrorist activities) appears as payee/endorsee/applicant and report of such transaction as and when detected to FIU, NRB.

6.3 Proliferation Financing

The provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Preventing proliferation financing is an important part of combating proliferation. It is essential to disrupt the financial flows available to proliferators and to obstruct and complicate the procurement of the illicit goods, services and technology needed for the development of weapons of mass destruction and their means of delivery. The Bank shall incorporate the procedures required for identification of any risks associated with Proliferation Financing in the SOP framed under this policy.

7. Legal Framework

7.1 International Perspective

Financial Action Task Force (FATF) 40 + IX Recommendations

The Financial Action Task Force (FATF) is an independent inter-governmental body established in 1989 by the ministers of its member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the financial system.
The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard. The FATF recognizes that the countries have diverse legal, administrative and operational standards and different financial systems, and so all cannot take identical measures to achieve the common objectives of countering the money laundering and terrorism financing threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances in order to:

- Identify the risks, and develop policies and domestic coordination;
- Pursue money laundering, terrorist financing and the financing of proliferation;
- Apply preventive measures for the financing sector and other designated sectors;

- Establish powers and responsibilities for the competent authorities and other institutional measures;
- Enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and
- Facilitate international cooperation

Asia Pacific Group on Money Laundering

The Asia/pacific Group on Money Laundering is an autonomous and collaborative international organization founded in 1997 in Thailand, consisting of 41 member nations and a number of international and regional observers. The members and observers of APG are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and financing of terrorism, in particular the 40 Recommendations as defined by the (Financial Action Task Force) FATF.

The core functions of APG include:

- Assessment of compliance of the APG members with the FATF standards on Money Laundering and Terrorism Financing through mutual evaluation
- Coordination and technical assistance and training to the member states
- Conduct research and analysis to enhance the understanding of the issues related to Money Laundering and Terrorist Financing.
- Contribute to the global AML/CFT policy formulation

7.2 National Regulatory Framework

The following are the applicable domestic laws and rules pertaining to the KYC and AML/CFT;

- Asset/Money Laundering Prevention Act 2008 (including amendments)
- Asset (Money) Laundering Prevention rules 2016
- Unified Directive issued by NRB
- Directives and Guidelines issued by FIU from time to time

The Nepalese AML/CFT regime provides for the various bodies with the specific mandated to each. They are Coordination Committee, Technical Committee, Financial Information Unit, and Assets Laundering Investigation Department.

The Legislation pertaining to the AML/CFT mandates the FIU to:

a. Receive and collect reports on suspicious and prescribed threshold financial transactions and other information relevant to money laundering and Financing of terrorist activities from government agencies, financial and non-financial institutions,
b. Analyze and assess information received from the reporting agencies,
c. Provide suspicious and relevant information to the investigation department and other relevant units,
d. Direct banks, Financial and non-financial institution regarding the reporting requirements,
e. Ensure compliance by reporting entities with regard to their obligations under the law, rules and regulations,
f. Inspect transaction and records of banks, financial and non-financial institutions,

g. Manage training and awareness programs
h. Take actions against banks, financial and non-financial institutions in case of non-compliance of reporting requirements, and
i. Develop information exchange mechanisms with other FIUs or related international institutions by entering into formal understandings or obtaining memberships

8. Bank's Effort to combat Money Laundering and Financing of Terrorism

8.1 Bank's Policy on KYC and AML/CFT

The Bank's policy on Know Your Customer and Anti Money Laundering / Combating Financing of Terrorism shall apply to all the branches, units and businesses of the Bank. This Policy shall be the benchmark for the supervision of systems and procedures, controls, training and other related matters in the implementation of the KYC guidelines in the Bank.

By the very nature of its functioning, banks are more susceptible to the risk of money laundering and the possibility of its various services being unwittingly used as conducting and cycling the ill-effects of the tainted/illegal money by the launderers. As an organization committed to the prevention of money laundering and terrorism financing activities, the Bank shall take following measures;

- Develop internal procedures and technology that assists the Bank in monitoring transactions for the purpose of identifying possible suspicious activities. Likewise, the Bank shall implement/use automated AML solution, database for effective KYC management, risk assessment, screening and transaction monitoring etc.
- The Bank will continue to update policies and procedures in line with the laws, regulations and regulatory guidelines. Compliance Department will be delegated the task of overseeing the Bank's policies, practices and procedures with regards to money laundering.
- The Bank will take all reasonable steps to ensure that Customer Due Diligence information is collected and up-to-date, and that identification information is updated in the event where the Bank comes to know about any changes with regards to the parties involved in the relationship.
- The Bank will take reasonable steps to verify the identity of the customers, including the beneficial owners of corporate entities, and the principals behind customers acting as the agents.
- The Bank shall ensure that the Internal Audit Department on periodic basis and Compliance Department randomly observe audit requirements of KYC guidelines and verification of its implementation at branches and other operational units of the Bank.
- The Bank shall not tip-off its customers regarding suspicious transactions and /or any internal/external investigation being carried on them.
- The Bank shall not maintain any relationship with shell companies.
- The Bank shall cooperate with any lawful request for information made by authorized government agencies/statutory bodies during their investigation.

- The Bank shall ensure that the training sessions on KYC and AML/CFT procedures and guidelines are included in the Training calendar of the bank on an ongoing basis. The Bank shall arrange to update and module these training sessions to make all the concerned fully understand the rationale behind the KYC and AML procedures and implement them consistently.
- In order to educate customers on KYC requirements and the need for seeking certain personal information from the customers/applicants for opening accounts and/or establishing any business relationship with the Bank, and as well to ensure transparency, the Bank shall publish this Policy in the Bank's website. It will be the primary duty and responsibility of Operational Staff to educate the customers and tactfully/convincingly explain the need for customer profile and its relevance in enabling the Bank/Branch to render better customer service.
- The Bank shall establish clear lines of internal responsibilities and reporting.
- The Bank shall pursue a zero tolerance on all matters related to AML/CFT compliance and shall take action for resolving issues in higher priority.

8.2 Bank's Framework of Anti Money laundering /Counter Financing of Terrorism

The standards of Know your customer and Anti Money Laundering/Counter Financing of Terrorism of the Bank are designed to facilitate the businesses and other support units meet their responsibilities in relation to the prevention of the activities related to money laundering and terrorist financing. These standards have been designed based on the relevant acts, rules and regulations, regulatory guidelines and the banking practices on prevention of money laundering and terrorism financing activities. Further, these standards will be reviewed based on the subsequent amendments in the relevant laws, rules and regulations, regulatory guidelines and recommendations.

The Bank's KYC and AML/CFT standards are based on the following 4 Pillars:

I. Customer Acceptance Policy;
II. Customer Identification Procedures;
III. Monitoring of Transactions ; and
IV. Risk Management

8.2.1. Customer Acceptance Policy (CAP)

Bank's Customer Acceptance Policy (CAP) lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship in the Bank broadly are:

- No account shall be opened in the name altering from the primary identity document, anonymous or fictitious (benami) name(s), blank names or CIFs/accounts with numeric/alphanumeric characters only.

- Accounts/CIF shall be opened only in the name of natural and legal person/organization, the name being the same as in the primary identity document of the person/entity. Accounts may however be opened with different account titles identifying the nature/use/purpose/type/ of account at the written request of the legal person/organization with appropriate control parameters.

Minimum required information and documents i.e. proper identification and information pertaining to the prospective client shall be obtained prior to account opening or performing business relation of any kind, as per the AML Act, AML Rule, FIU Directives, NRB regulations/Directives and as per the product paper/policy/guidelines set forth by the Bank.

- Necessary checks are done before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. No account is opened where identity of a customer/prospect matches with any person or entity in the sanctions lists (domestic and International).

- Not to maintain account relationship or conduct any kind of banking transaction (except for deposit to the respective blacklisted customer's account) with the individuals/entities blacklisted by CIB, Nepal until release from the list.
- Not to open an account, where the staffs designated to open new accounts, find sufficient ground that the identity of the prospective customer could not be verified and/or the prospective customer is not disclosing the required identity, the reason for opening account, transaction frequency and volume, etc. and any other information deemed necessary for account opening. The refusal shall be properly documented and communicated to HO AML/CFT Compliance Officer through Branch AML/CFT Compliance Officer.

  Further, the Bank shall freeze an existing account under the situation where the designated staff is unable to apply appropriate customer due diligence measures i.e. unable to verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data /information furnished to the Bank. Decision for closure of such accounts shall be approved by Senior Management level official under recommendation of AML/CFT Compliance Officer at HO and also after giving due notice to the customer explaining the reason for such decision. Closure of such accounts shall be informed to FIU in written.

- The Bank shall not establish any business relationship with the shell companies and the institutions that deal with shell companies. Any identified business relationship with the financial and other institutions that allow the transaction of shell bank, will be discontinued.

- The Bank shall not be associated with any entity located in the jurisdictions identified by the FATF as "FATF blacklist" or those fully sanctioned by the agencies that the Bank refers to like, UN, OFAC, HMT, EU etc. Further, special attention shall be given for

conducting any transactions involving individuals/entities located in the jurisdictions under "FATF Grey list" and under sectoral sanctions by the sanctions imposing agencies. Prior approval from executive level authority within the functional structure shall be obtained for the same.

- The Bank shall not offer services like payable-through accounts and nested accounts services to its respondent Banks/FIs while offering correspondent banking services to the Banks and FIs.

- Implementation of CAP should not be too restrictive resulting in denial of banking services to the general public, especially those who are financially or socially disadvantaged.

- The decision to open an account for Politically Exposed Person (PEP) and Person in Influential Position (PIP) shall be approved by Senior Management Level official. Information of such account shall be provided to the AML/CFT Compliance Officer at HO.

8.2.2. Customer Identification Procedures (CIP)

Customer Identification Procedure means undertaking client due diligence measures including identifying and verifying the customer and the beneficial owner. The first requirement of knowing the customers for anti-money laundering purposes is to be satisfied that a prospective customer is who he/she claims to be. The second requirement of knowing the customer is required also to ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake or any expected, or predictable pattern of transaction, which would enable the Bank in risk profiling of the customer.
Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information to the Bank's satisfaction and also to satisfy the competent authorities that the due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

The Customer Identification procedures are to be carried out at the following stages;

- While establishing a banking relationship; onboarding of the account relationships
- When the Bank feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account;
- When any customer (non-account holder) conducts a transaction with the Bank, greater than the thresholds specified by the regulatory
- when bank sells third party products as agent;
- when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data;
- Customer identification will also be carried out in respect of non-account holders approaching bank for high value one-off transaction as well as any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Bank.

While identifying the natural person or legal person, the bank shall obtain the documents, data and information as prescribed in the Bank's procedural guidelines. All the documents and information pertaining to the identification of the natural and legal person should be retained in a legible manner and in the managed way. The Bank shall require identifying the legal persons or legal arrangement by understanding nature of business and its ownership & control structure. The Bank shall further verify the identity of legal person or legal arrangement through information such as name, legal form, proof of existence, binding & regulating power and registered address. The Branch AML/CFT Compliance officer in the branch shall verify that any person purporting to act on behalf of the legal person/entity is so authorized & identify/verify the identity of that person. The Bank may deploy a specialized central unit to facilitate and streamline the customer identification process and proper recording of the customer information in digitized form.

8.2.2.1. Identification of Customer through e-KYC and Non face to Face Customer

While establishing an account based relationship with individual customer, the Bank shall make necessary verification so as to ensure that only one customer identifier number is assigned to the respective customer. Biometric Based e-KYC authentication can be done by the Bank for the natural person. The Bank may deploy e-KYC both for online based account opening and updating the existing customer information. However, use of e-KYC for onboarding the Institutional Customers shall be prohibited. The Bank shall develop separate guiding document for e-KYC process & procedure.

Accounts opened using e-KYC, in non-face to face mode are subject to the following conditions:

- There must be specific consent from the customer for authentication through OTP.
- The customer should qualify for Basic due diligence standards set by the Bank. However enhanced due diligence standards set by the Bank to be conducted for PEPs & High-risk customer.
- Email address and contact number shall not be subject to waiver for such customers.
- Form (e-KYC) for updating existing customer information shall mandatorily include Existing accounts number, Mobile No, Email address of customer.
- A declaration shall be obtained from the existing customer to update information that all information provided/updated is true & correct and customer shall provide related additional documents to the Bank if deemed necessary.
- The Bank shall have monitoring procedures including systems to generate alerts for such e-KYC based accounts in case of any non-compliance/violation, to ensure compliance with the above mentioned provisions.

It is recognized that electronic transactions and services are convenient. Customers may use the internet or alternative means because of their convenience or because they are not able to visit branch in person. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for money laundering. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification.

The Bank shall pay special attention to any money laundering patterns that may arise from non-face to face customers or transactions that favor anonymity and be used to facilitate money laundering; hence the Bank shall take appropriate measures to treat with such patterns. The Bank shall monitor the transactions on customer's account opened through online platform to identify any unusual pattern or behavior to facilitate money laundering. Hence the activities of accounts open through online platform are monitored by the bank for abnormal increase or change in the defined threshold and number of transactions or transactions that favor anonymity and report any suspicious activities based on same to FIU, NRB or categorize customer under the watch list category on the KYC/AML Screening Application.

The Bank shall incorporate the procedures required to address any money laundering risks associated with non-face to face business relationships or transactions in the SOP framed under this policy.

8.2.2.2. Customer profiling and Risk based Customer Due Diligence

(a) Bank shall prepare a profile for each new customer based on risk categorization. In general, Risk categorization should take into account the following risk variables specific to a particular customer or transaction:

- Information relating to customer's identity, social/financial status
- The purpose of account or business relationship
- Nature and size of transaction undertaken by the customer
- Type of product/service availed by the customer
- Country or the Jurisdiction where the customer or customer's business is domiciled
- Beneficial owners of the customer
- Level of regulation or governance regime to which a customer is subjected to
- Duration of relationship with the customer and regularity / trustworthiness of the customer
- Knowledge of local laws, rules and regulations, structure and extent of regulatory oversight
- Transparency and Disclosure requirements
- Intermediaries and business partners of the customer
- Countries National and Sectoral Risk Assessment Reports as available
- Investigation Reports of Distinguished International organizations working in the fight against money laundering and financing of terrorism.

(b) Based on the above criteria, Bank shall categorize its customers into low risk, medium risk and high risk category based on its assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to. The nature and extent of due diligence, may be based on the following principles:

(i) Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, is categorized as low risk. Illustrative examples include pensioners, people belonging to lower economic strata, government departments and government owned companies, regulators and statutory bodies, etc. Bank shall perform Simplified Due diligence of low risk customer. Where any suspicion of money laundering and terrorism financing have been detected, such accounts shall be categorized as high risk and enhanced customer due diligence shall be conducted, and further, reported as suspicious to HO AML/CFT Compliance Officer.

(ii) Customers who are likely to pose a higher than average risk are categorized as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Bank shall perform Basic Due diligence of medium risk customer.

(iii) Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, accounts of bullion dealers (including sub-dealers), jewelers and Politically Exposed Persons (PEPs) of domestic or foreign origin etc. are categorized as high risk. Bank shall perform Enhanced Due diligence of high risk customer.

Other customers to be categorized as high risk are:

a) Non-resident customers (except Nepalese and Indian Nationals);
b) High net worth individuals;
c) High Cash Incentive Businesses
d) Trusts, charities; NGOs and organizations receiving donations and no periodic financial audits are performed;
e) Politically Exposed Persons [PEPs] of domestic and foreign origin; customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner,
f) Customers of countries identified to have higher risk of corruption, tax evasion and other criminal activities. (For this purpose, the Bank shall take into account the top 10 most High Risk Countries as published by the BCBS– Basel AML Index Report) and countries listed on FATF-Jurisdictions under increased monitoring;
g) Close associates of Politically Exposed persons (PEP) and
h) Those with dubious reputation as per public information available etc.

(iv) The risk assigned to an existing customer may undergo change depending on the change in risk parameters of the customer based on various risk indicators, like, customer type, customer behavior, profession, nature and scope of business, product type, volume and nature of transaction, beneficial owners, transaction partners, etc.

(v) In addition to what has been indicated above, Bank shall further define the detail procedural guidelines to take steps to identify and assess the ML/TF risk for customers, countries and geographical areas as also for products / services /

transactions / delivery channels and will frame controls and procedures to effectively manage and mitigate the risk adopting a risk-based approach.

(vi) The Bank shall not open the account, commence business relations or perform the transactions where they are unable to apply appropriate customer due diligence measures. Such situation the bank shall consider for filing suspicious transaction report in relation to such customer.

8.2.2.3. Ongoing customer Due Diligence and periodic review

Customer Due Diligence information shall be regularly reviewed, even after the completion of account opening or the commencement of any kind of relationship with the customer. The frequency of review shall be based on the level of risk associated with the kind of relationship maintained by the customer and such review will be recorded in the concerned customer file. High risk customer relationship and transaction of high volume and close to threshold, for instance, will be reviewed at more frequent intervals than the medium and low risk relationships. Existing customers shall be screened against updated PEP & sanction list database maintained by the Bank as part of ongoing due diligence.

Any shortcomings in CDD information detected in the review must be regularized as soon as possible. Additional information should be taken about the existing customers where it is apparent that the existing CDD information is out of date or inadequate.

Any information on changes in nature and volume of transaction, changes in nature and scope of business operation, change in ownership and/or change in person controlling a relationship, information on identified beneficial owner, or any other identified worthy alteration can be taken as a trigger update CDD information of the customer.

Bank shall not insist on the physical presence of the customer for the purpose of furnishing information or furnishing consent for authentication/verification of information supplied unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, in the course of ongoing due diligence, the documents and information of the customer obtained through any reliable means shall be acceptable.

Bank shall undertake Customer Due Diligence measures when establishing business relationship. For the purpose of monitoring the high risk accounts for which the bank has to conduct enhanced due diligence, for all cash transactions of NPR 1 million and above, sufficient declaration of source of fund shall be obtained from the customer. However, for all cash deposit transactions of NPR 5 million and above, declaration of sources of fund shall be obtained, along with the supporting document of the declared sources, as far as possible. . Further, where daily transactions (either sum of total debit or sum of total credit) in a high risk account equals or exceeds NPR 10 million, purpose of conducting the transaction shall also be obtained from the customer, as far as possible. Any suspicion detected in the account activities shall be immediately reported to HO AML/CFT Compliance Officer.

Bank shall conduct due diligence immediately irrespective of AML risk rating, If transaction conducted by the customer does not commensurate with personal and financial profile of the customer. If there is sufficient ground for suspicion in regards to the accuracy and adequacy of the information & documents submitted by the customers.

The operating procedures framed under this policy shall summarize the CDD requirements and identification standards for the customer categories across the Bank. For any customer category, whether or not specified by such guidelines, CDD requirements and identification procedures must be in line with this policy document and the regulatory guidelines.

8.2.2.4. Due Diligence of Vendors/Service Providers/Business Partners

The Bank shall conduct Due Diligence of its vendors, service providers, and other business partners in alignment with the KYC norms from the perspective of AML/CFT. Appropriate measures shall be taken to ensure that the third-party relationships do not pose significant money laundering and terrorism financing risks to the Bank. The procedural measures formulated under this policy shall incorporate the due diligence standards for the following third party relationships of the Bank:

- Listed vendors and service providers from whom the Bank makes necessary procurements, rents the space and avails services as per the Bank's procurement by laws and guidelines
- Firms, individuals, institutions and companies hired by the Bank for consulting services
- Individuals, firms, companies and organizations entered into contract by the Bank for performing specific job on behalf of the Bank as a third party agent and/or the business partner
- Financial or non-financial entities that the Bank establishes any kind of business relationships during its operation

The Bank shall collect information about the potential business partners through direct contact, basic internet searches and database checks, input or supervision from an independent business function of the Bank and assistance from any reliable external sources if deemed necessary.

The Bank shall deny maintaining any kind of relationship with the third party where;

- The party is not able to prove its legitimacy
- The party present false, misleading or incorrect information to the Bank
- The party wants to work without a contract or with a vague contract that do not meet the minimum standards as defined by the Bank
- The party refuses or is hesitant to provide any documentation required by the Bank regarding the disclosure of identity, nature and scope of its business and its beneficial owners
- The party requests for any indirect and unusual payment or billing procedure like payment to anonymous bank account, payment through shell companies, payment through foreign bank accounts other than the country where the services are being performed, payment in high value cash or through bearer cheque, etc.

- The party in any way (directly or indirectly) is incorporated in a jurisdiction identified by FATF to be a non-cooperative jurisdiction.

8.2.2.5. Identification of PEPs (Politically Exposed Persons)

Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a country e.g. Heads of states/Governments, senior politicians, senior government/judicial/military officers, senior executives of state owned corporations, important political party officials, etc. The Bank shall have the option of establishing a relationship with PEPs provided that:

- Sufficient information including the sources of fund, family members and close relatives is obtained on the PEP.
- The identity of the person shall have been verified before accepting the PEP as a customer
- Prior approval has been taken from Senior Management Level official for opening the account of PEP
- Accounts of PEPs shall be subject to enhanced monitoring on an on-going basis. In the event of an existing customer or a beneficial owner with significant control of an existing account is known to be a PEP or subsequently becoming a PEP, approval from Senior Management Level official shall be obtained to continue a business relationship.
- The account of PEPs and their family members and close relatives as far as identified, shall be subject to enhanced CDD measures including enhanced monitoring on an on-going basis.
- PEP screening of family members as well as close associates shall be done on the basis of information provided in account opening form of prospective customer.

The instructions as above shall also be applicable to any account(s) where PEP is identified to be a significant beneficial owner.

In order to ensure that the Bank's customers and prospects are adequately identified regarding whether or not he/she falls under the PEP category, the Bank may develop its own list of PEPs or alternately the Bank may procure/use the PEPs list databases provided by various authorized and/or dedicated vendor from among those providing service in the Nepalese market.

Delisting of PEPs

For the purpose of fulfilling KYC and due diligence requirements as per this policy, any individual identified to be PEP shall remain as PEP at least for the period of 5 years from the complete release of the prominent position. Thereafter the Bank shall have the authority to release any individual from the PEPs list depending upon the current profile of the person and significance of the person to remain as a PEP. Compliance Officer and/or the officials designated by the Compliance Officer of the Bank shall have the authorities to decide on

whether or not any person shall remain to be identified as PEP after release from a prominent position as defined through National AML legislations.

8.2.2.6. Identification of Sanctioned Entity

The Bank shall adopt appropriate measures to monitor effectively the compliance with AML legislation, rules and regulations governing the freezing of funds and assets of the sanctioned person/entity, specifically the sanctions list of individuals and entities circulated by the Ministry of Home Affairs (Nepal), UNSCR, OFAC, EU and HMT. The Bank shall ensure effective implementation of a dedicated sanctions list databases from the dedicated service provider so as to ensure that no relationship is being maintained with any sanctioned entity.

Any prospect customer or the customer before onboarding or during ongoing due diligence or initiating cross border transactions including wire transfers, should be scrutinized against the sanctions list databases maintained by the Bank.

Any customer/prospects of the Bank if identified/suspected to be a sanctioned entity, shall be reported to FIU through AML/CFT Compliance Officer, by freezing of funds and postponing any relationship with the Bank until further instruction from the regulator.

8.2.2.7. Adverse Media Screening

Adverse media screening, also known as negative news screening, involves searching for negative news about a person or business i.e. the interrogation of public data sources and third-party data sources for negative news or broadcasts associated with an individual or company, for proactive customer risk management in terms of mitigating the risk of money laundering and terrorism financing. The adverse media screening shall include the following:

- All the prospects and existing customer shall be subject to screening against the adverse media screening databases and public data sources
- The Bank may procure and implement a dedicated adverse media screening tool and databases from the authorized vendors/third-party from among those available in Nepal
- The screening results shall be reviewed in order to confirm the matches
- If the matches are confirmed, the customer shall be assigned a high risk rating depending on the nature of adversity. Further, the account may even be debit restricted, if deemed necessary, and the report of same shall be submitted to FIU, NRB.
- In case of confirmed prospects, the Bank may turn down the request to maintain any kind of relationship with such, depending on the adversity of the new.
- AML/CFT Compliance Officer and/or designated officer shall extend necessary coordination to the screening units where adversities have been escalated for further clarification and further course of action.

8.2.2.8. Identification of Beneficial Owners

When a customer is acting (or appears to be acting) on behalf of others, sufficient evidences on identification of both the parties (i.e. agent and the principal agent) must be obtained. The Bank shall take all reasonable steps to verify the beneficial owner of the customer account

and/or business relationship at the time of initiating or in due course of business relationship with account holder, any person or individual conducting any transaction or maintaining any kind of relationship with the Bank in favor of the account holder or any other customer. Where the customer is a legal person, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means that may include right to appoint directors or to control management or policy decisions through voting agreements, shareholders agreements etc.

The Bank shall identify and obtain KYC information of the beneficial owners where;

- The beneficial owner is the relevant natural person holding 10 percent or more shares or has obtained voting right.
- The beneficial owner is the relevant natural person who holds the position of senior management official in an organization/institution.

Following measures shall be considered for identification of a beneficial owner:

a. Obtain relevant information from the customer or obtain self-declaration of the customer
b. Publicly available information regarding the customer
c. Analyzing the information available in social media
d. Obtain Information from the Legal records maintained as per prevailing laws
e. Available Databases of business and profession
f. Obtain information from the related government organization if needed

Where the customer is a trust or similar type of organization, the identification of beneficial owner(s) shall be the identification of the author of the trust, the trustee, director, the beneficiaries and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

Where the customer or the beneficial owner is the company listed on a stock exchange, or is a subsidiary of such company, or is foreign company listed in stock exchange being regulated by the regulatory authority of the country known to have adequately implemented the international standards on money laundering and terrorism financing, it is not necessary to identify and verify the identity of any shareholder or the beneficial owner of such companies. Documents and all the records related to the beneficial owners shall be kept safe for the period of 5 years from the date of termination of relationship or transaction.

8.2.2.9. Identification in Wire Transfers

Wire transfers are used as an expeditious method for transferring funds between bank accounts. As wire transfers do not involve actual movement of currency, they are considered as a rapid method for transferring value from one location to another. Prior to initiating wire transfers of any amount in any currency, the bank shall obtain following information at minimum, with the customer.

i. Originator's Name,
ii. Originator's Account number or in case of non-account holder, a separate transaction identification code or , a unique transaction reference number which permits traceability of the transaction

iii. Originator's address or birth date and birth place or citizenship number or national identity card number or customer identification number
iv. Beneficiary's name and account number or in case of non-account holder, a separate transaction identification code of the beneficiary a unique transaction reference number which permits traceability of the transaction.
v. Any other information as specified by the regulatory authorities

Where, the wire transfer is below NPR 75,000.00, the information as per above clause no. iii may not be necessary to obtain. However, the waiver authority of such information shall remain with the Branch Manager or above level. Before exercising the waiver, the authority shall ensure that the country of the originator is compulsorily available, is not from the sanctioned jurisdictions and may verify the information where there is a suspicion of ML/TF. Wire transfers, where any information as defined in above clause no. 'i' and 'ii' could not be obtained or is not available to the Bank, the Bank shall not pay out such wire transfers.

Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file should contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and the Bank shall include the originator's account number or unique transaction reference number.

The details as specified above for cross border wire transfer shall not be necessary to obtain for domestic wire transfers in following cases:

i. Where the originator and beneficiary is the existing account holder of the bank with no KYC deficiency and is perceived to have low risk of money laundering and terrorism financing.
ii. Where wire transfers are conducted through cards as a result of payment of procurement of goods or services and details of such transactions are adequately recorded in the statement of debit card, prepaid card, credit cards, etc.
iii. Where the fund has been transferred across accounts of the same originator/beneficiary within different financial institutions

Inter-bank transfers and settlements where both the originator and beneficiary are banks and financial institutions would be exempted from the above documentation requirements.
Wire transfer is an instantaneous and preferred route for transfer of funds and hence, there is a need for preventing launderers and criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse.

The Bank shall retain basic information about the originator of the wire transfers as stated above and make available to the appropriate law enforcement and prosecutorial authorities when asked for in order to assist them in detecting, investigating, prosecuting launderers and criminals and tracing their assets.

The Bank shall perform name or sanctions screening of the customer and all related parties to the wire transfer transactions as well as sanctions screening of the payments or swift messages related to the trade finance transactions.

The Bank shall ensure that wire stripping activities are not being conducted in the transfer messages/payments such that full compliance is been ensured to block payments linked with the sanctioned individuals, entities and countries. Resubmission of any transaction previously rejected due to any concerns over sanctions, shall be denied and records of such transactions rejected and any attempts of resubmission, shall be maintained by the concerned department. Necessary control mechanism and approaches shall be formulated to ensure that wire stripping activities are prevented.

The Bank shall obtain true identity of the beneficiary while making payment of the wire transfers. All the wire transfers must be accompanied by accurate and meaningful originator and beneficiary information.

The Bank shall retain in record all the information and document related to wire transfers at least for 5 years from the date of transaction. Where the staff, initiating the wire transfer has reason to believe that a customer is intentionally structuring the wire transfers to below threshold limits to several or same beneficiaries in order to avoid documentation or reporting requirement, the bank shall insist on complete originator and beneficiary identification before effecting the transfer. Where the customer is not cooperative, the Bank shall make necessary efforts to establish the identity and report suspicious transaction report (STR) to the Financial Information Unit.

8.2.2.10. Identification in Cross border Correspondent Banking

Correspondent banking is the provision of banking services by one Bank (correspondent bank) to another Bank (the respondent bank).
Following measures shall be taken by the bank while maintaining cross border correspondent banking relationship

- Correspondent banking relationship shall be established only after the approval of Senior Management Level official.
- The Bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing due diligence measures so as to ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.
- The Bank shall not establish correspondent banking relationship with 'shell banks' and shall further ensure that the respondent bank do not allow the operation of accounts by the shell bank.
- The Bank shall ensure that the respondent banks have adequately in place the anti-money laundering policies and procedures and apply adequate due diligence procedures for transactions conducted through the correspondent accounts.
- On the basis of publicly available information, the Bank shall be familiar with the reputation of respondent bank, its supervision standards, and should identify whether or not the respondent bank has been under investigation and/or regulatory action in regards to money laundering and financing of terrorism activities. The information in this regard shall be properly maintained in the respondent bank profile.

- Correspondent Banking Services of the Bank shall be restricted of any payable-through services and nested services for direct access by the customer or the underlying third party of the respondent Banks/FIs.

8.2.3. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC/AML procedures. Bank will exercise ongoing due diligence with respect to every customer and closely examine the transactions to ensure that they are consistent with the customer's profile and sources of funds as per extant instructions. The ongoing due diligence is based on the following principles:

a) The extent of monitoring depends on the risk category of the account. High risk accounts have to be subjected to more intensified monitoring.

b) Bank will pay particular attention to the following types of transactions:

   i. Large and complex transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.
   ii. transactions which exceed the thresholds prescribed for specific categories of accounts.
   iii. transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.
   iv. High account turnover inconsistent with the size of the balance maintained.

c) Bank shall closely monitor the transactions in accounts of Individual or firms. In the accounts where there are multiple small deposits (generally in cash) and multiple withdrawal (generally in cash) near to the threshold amount defined by regulator across the country in one bank account, the operations in such accounts will be analyzed and in case any unusual operations or suspicious transactions are noticed in the accounts, the matter will be immediately reported to FIU, NRB. The Bank shall implement a dedicated Monitoring Software for automated monitoring of customer transactions in order to identify the transactions of suspicious nature.

d) Special attention shall be given to business relationships and transactions with persons from or in countries identified by FATF to insufficiently apply the FATF recommendations or identified to be non-cooperative in the fight against money laundering and financing of terrorism.

e) Bank shall monitor the transactions on customer's account opened through online platform to identify any unusual pattern or behavior to facilitate money laundering. Hence the activities of accounts open through online platform are monitored by the bank for abnormal increase or change in the volume and number of transactions or transactions that favor anonymity.

8.2.4. Internal Control and Risk Management

Bank will exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with its knowledge about the clients, their business and risk profile and where necessary, the source of funds. Bank shall also ensure that, before launching of new products and services or modifying the existing features, formulation and implementation of necessary procedures and guidelines, reasonable measures are being taken to identify and assess money laundering and terrorism financing risks being posed by the products and services and its inbuilt features, nature of transactions and delivery channels, procedural guidelines, etc under concurrence from Compliance and Corporate Governance Department to manage and mitigate the identified risks and comply with the KYC and AML/CFT legislations.

8.2.4.1 Internal control system

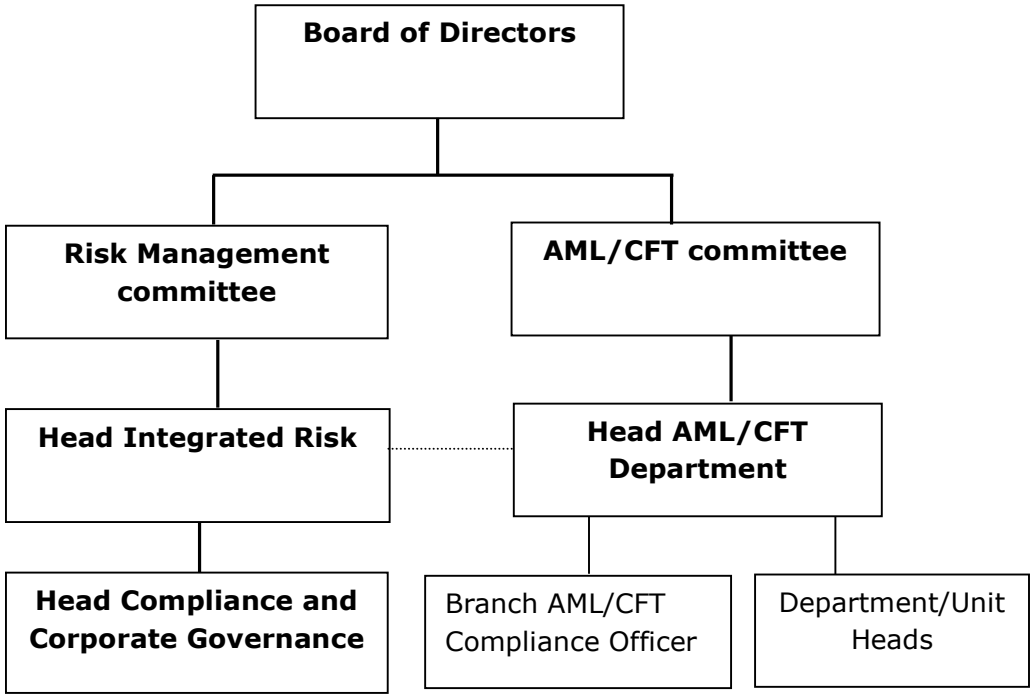
8.2.4.1.1 AML/CFT Department and AML/CFT Compliance Officer

The Bank shall have a separate AML/CFT Department headed by the AML/CFT Compliance Officer designated by the Bank as per the AML regulatory guidelines who will directly report all the matters on anti-money laundering and counter financing of terrorism to the Board level AML/CFT committee. The Bank will assign the responsibility of AML/CFT compliance Officer to the Managerial level staff at Head Office to function as a focal point for implementation and compliance of this Policy and guidelines formulated to execute this Policy in practice. The AML/CFT compliance officer designated by the Bank in this regard will have overall responsibility for maintaining oversight and coordinating with various divisions/departments in the implementation of KYC and AML/CFT policy. However, primary responsibility of ensuring implementation of this policy and related guidelines will be vested with the respective Branches/Divisions. Branch AML/CFT Compliance officer would ensure proper implementation and reporting, as per provisions of this policy, to the AML/CFT Compliance officer at Head office, that will be the Head of AML/CFT Department, who will be responsible for following major duties though are not limited and to comply/get it complied with all the regulatory provisions and legal KYC and AML/CFT standards:

- Overall monitoring of the implementation of the Bank's KYC and AML/CFT policy
- Ensuring that proper KYC mechanism is implemented as per prevailing laws and regulations
- Ensuring that records are kept properly in regard to KYC and AML/CFT Policy of the Bank
- Monitoring and reporting of transactions, and sharing of information, as required under the law
- Interaction with Branch AML Compliance Officers at branches for ensuring full compliance with the Policy
- Timely submission of Threshold Transaction Reports (TTRs) and Suspicious Transaction Reports (STRs) to FIU

- Maintaining Liaison with the government agencies, regulating authority, FIU, 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 Executive Management/AML/CFT Committee/Board
- Train/Educate staffs on KYC and AML/CFT compliance issues through dissemination of relevant specified guidelines and circulars, rules, regulations, notices, standards, manuals, internal codes of conduct.

The reporting line of authority for issues pertaining to KYC and AML/CFT compliance shall be as postulated in the following diagram.



Head of AML/CFT Department, the AML/CFT Compliance officer, shall be responsible for the general oversight of the Bank's KYC and AML/CFT Policy, effectiveness of control, monitoring and reporting procedures and to establish and maintain adequate arrangements for training on KYC and prevention of money laundering and terrorism financing. The obligation of AML/CFT Compliance Officer designated pursuant to sub-section (3) of section 7(P) of Asset (Money) Laundering Prevention Act 2008, as prescribed in the subsection (4) of section 7(P) is as follows:

a. Function as focal point to perform tasks in accordance with the Act, these Rules and the Directives,
b. Cause to maintain secure record of transaction,
c. Provide information about suspicious or other necessary transaction to the Financial Information Unit through letter or electronic means of communication like fax, email,
d. Provide information about transaction of the branch offices to the Financial Information Unit in a regular basis.

The details of AML/CFT compliance Officer including name, designation, address, qualification, contact number, email etc. shall be furnished to FIU and information regarding the change in AML/CFT Compliance Officer and details thereof shall also be furnished to the FIU.

AML Unit at Central Level:
AML Unit at Central level shall reside within the AML/CFT department at Head Office. Monitoring and analysis of AML alerts, including the sanctions information in SWIFT's Sanction Screening Portal, shall be done at the centralized AML Unit on a daily basis. Makers/checkers at Centralized AML Unit will analyze alerts pertaining to their respective assigned branches on day to day basis and will close the alerts after thorough analysis of the transactions/alerts and ensure that all the transactions are genuine in nature and match with the business profile of the customer known to the Bank. STRs on all suspicious transactions shall be put up to the AML/CFT Compliance Officer immediately for recommendation and further approval and onwards submitted to the FIU, NRB through the AML/CFT Compliance Officer.

8.2.4.1.2 Branch AML/CFT Compliance Officer

AML/CFT Compliance Officer at HO will have overall responsibility of maintaining oversight and coordinating with various divisions/ departments in the implementation of KYC and AML/CFT policy. However, primary responsibility of ensuring implementation of KYC and AML/CFT policy and related guidelines/procedures will be vested with the respective branch/division. For this purpose, a staff will be designated from each branch as Branch AML/CFT Compliance Officer who would ensure proper implementation and reporting, as per the provisions of this Policy, to the AML/CFT Compliance Officer at HO. Where separate Branch AML/CFT Compliance Officer is not designated, Operation Officer, or the staff officiating the said position will be assuming the responsibilities of Branch AML/CFT Compliance Officer. The Branch AML/CFT Compliance Officer shall have a direct reporting line to the AML /CFT Compliance Officer at Head Office for all KYC and AML/CFT related issues.

8.2.4.1.3 Internal Audit Department

Bank has entrusted Internal Audit Department with the responsibility to test the implementation and adherence of Bank's KYC and AML/CFT policy and procedures. As a part of the Internal Audit Plan, the Bank's Internal Audit will provide an independent evaluation of implementation status of KYC and AML/CFT policy including legal and regulatory requirements. Internal Auditor shall specifically check and verify the application of KYC and AML/CFT procedures at the branches and comment on the lapses observed in this regards.

The findings/recommendations should be reported directly to the AML/CFT Compliance officer and the Audit Committee.

8.2.4.2 Risk Management

8.2.4.2.1 Risk Based Approach

Risk management is the process of identifying risk and developing policies and processes to minimize and manage risk. This requires the development of a process to identify, assess, prioritize, mitigate, manage and monitor risk exposures. A Risk based approach is a process that helps to identify potential high risks of money laundering & terrorist financing and develop strategies to mitigate them. Following are the steps applicable under Risk Base Approach:

A. Identify the existence of risks

- **AML/CFT Self-Assessment**

  It is the self-evaluation methods use by the bank to identify the level of risk in particular area of operation and business activities. As an exercise of Self-assessment, Compliance department has administered a self-assessment AML/CFT Questionnaires regarding roles of the Board of directors to implement compliance policy/procedures, sufficiency of management information systems, status of customer due diligence, effectiveness of compliance risk management, internal controls, compliance issues raised by Internal, External and NRB audit, AML/KYC norms, role, training and human resources perspective, record keeping, monitoring and reporting of suspicious activity etc. to identify and assess the level of compliance with reference to different laws, rules, regulations, policies, provisions specified in NRB Unified directive no.19 and other standards of AML/CFT compliances. Further Compliance department prepare the activities report for review of activities undertaken by AML/CFT department in compliance with regulatory requirements, AML laws & regulation and the Bank's internal policy & procedures.

- **Audit reports**

  Internal/External audit reports contain elements of an independent assessment that helps to identify events of possible non compliance. Further the scope of Internal audit shall assess the adequacy & efficiency of internal controls related to anti-money laundering & terriost financing functions as per the requirements of NRB guidelines.

B. Undertake assessment/measurement of risks

Once the Bank has identified the risk, the second step of the risk assessment/evaluation process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess ML/TF risk.

- **Inherent Risk**

  Inherent risk refers to the risk that exists before the application of controls or mitigation measures. The bank shall assess the risks inherent in its business, taking into account risk factors including those relating to its customers, countries or geographical areas in which it operates products & services, its transactions and delivery channels. In order to identify bank's inherent risks, assessment across the specific inherent risk categories is commonly undertaken, although other factors may also be considered. The following are more specific inherent risks which need to monitor /control and mitigate them effectively:

a) Geography/Country Risk

Country risk is the assessment of a country's or jurisdiction's vulnerability to money laundering, terrorism financing and targeted financial sanctions. Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. Country risk is not solely related to the country of origin of a customer.

The Bank shall take into account that a customer may have business interests to a country that may signify that the customer should be placed in a high risk category. The Bank shall identify domestic and international geographic locations that may pose a higher risk to AML/CFT. Each case should be evaluated individually when assessing the risks associated with doing business, such as opening accounts or facilitating transactions, in certain geographic locations. Following factors shall be considered for country risk assessment:

- Countries having inadequate AML-CFT systems/ Non-Cooperative Jurisdictions.
- Countries subject to sanctions, embargos or similar measures issued by UN, OFAC, EU, HMT and FATF.
- Countries identified by credible sources as providing funding or support for terrorist activities & proliferation of mass weapon and having significant level of corruption or other criminal activities.

b) Customer Risk

ML/TF customer risk considers the vulnerability that customers may be involved in money laundering or terrorist financing activities. ML/TF customer risk is significantly influenced by the nature and/or attributes of a customer. The bank shall determine, based on its own criteria, what risks a particular customer poses. Certain customers and entities may pose specific risks depending on the nature of the business, the occupation of the customer, the nature of anticipated transaction activity as prescribed based on the KYC/AML policy and regulator guideline. Following factors shall be considered for customer risk assessment:

- Implementation of customer due diligence measures as defined in the bank's SOP for KYC and AML.
- Implementation of customer acceptance procedures, customer identification procedures and reporting requirements as defined in the bank's SOP for KYC and AML.

- Categorization of customer accounts under High, Medium and Low risks.

c) Product & Service Risk

ML/TF risk is significantly influenced by the nature and/or attributes of products and services. Product / service risk is determined by whether the attributes of a product or service offer features or characteristics that can be used to facilitate money laundering and/or terrorist financing. Following factors shall be considered for product & service risk assessment:

- The bank shall duly consider AML risk factor while designing the risky product.
- The bank shall have adequate policy regarding AML CFT compliance that covers monetary instruments.
- Products or services which allow a customer to readily convert cash into monetary instruments or move value from one jurisdiction to another jurisdiction and which conceal the source of those funds shall be classified as high risk product.

d) Delivery Channel Risk

ML/TF risk is significantly influenced by the nature and/or attributes of the channels used to deliver products and services to customers. Channel risk is determined by whether the delivery of a product or service involves face to face contact with the customer, as face to face contact limits the ability for customer anonymity and facilitates establishing whether the customer is who they are claiming to be. The use of third parties as part of the delivery chain of a product or service also creates a higher ML/TF channel risk. Following factors shall be considered for Delivery channel risk assessment:

- Specific guidelines for establishing and maintaining business relationship with non-face to face customers shall be as per Bank's SOP for KYC & AML/ CFT.
- Due Diligence measures for correspondent banking shall be carried out as mentioned in the Bank's SOP for KYC & AML/ CFT.
- Reviewing the AML/CFT KYC status of the third party agencies to ensure the AML/CFT requirements.

C. Develop the strategies to monitor & mitigate identified risks.

The Bank shall develop the strategies & mitigating controls in form of AML/CFT policies, procedures and program .Such controls are assessed for each business line and enterprise-wide in terms of design, operating effectiveness and measuring the exposure to M L/TF through an assessment of the mitigating controls. The bank shall apply the following mitigating controls:

Formulation of annual program which includes all the aspects and specific activities to be performed in the given fiscal year period so as to identify, measure, monitor and control AML/CFT risks throughout the Bank.

- Conducting Training & Awareness program in the scope of KYC & AML/CFT.
- Implementing the Front Line Preventing Control as the foundation for minimization of KYC & AML/CFT risk in the Bank as a whole.

- Effective adherence to AML/CFT Roles & Responsibilities.
- Compliance to the Bank's KYC & AML/CFT policies and procedures.

9 Reporting Requirements to FIU

9.1 Threshold Transaction Reporting

NRB have specified threshold transaction limit for transactions including deposit, withdrawal, currency exchange, payments, transfers, etc. conducted through the Bank. Threshold Transaction Reporting (TTR) shall incorporate all the transactions conducted at or above threshold limit within a day or as specified in the guidelines/directives issued by the regulatory bodies from time to time.
The Threshold Transaction may be a single transaction or a sum of multiple transactions equaling or exceeding the threshold limit. Adequate sources of fund shall be obtained and recorded by the Bank for each threshold transaction that is equivalent to or exceeds the threshold limit as specified from time to time. The Bank shall submit Threshold Transaction Report in the format as prescribed in the regulatory guidelines within the specified deadline. AML/CFT Compliance Officer and/or the designated officer shall ensure that the Threshold Transaction Reports are duly submitted to FIU, NRB also in a digital form through goAML application.

9.2 Reporting of Suspicious Transaction/Activity

Whilst all unusual transactions are not automatically linked to Money Laundering, unusual transactions become suspicious if they are considered inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account. The AML Act 2008 (including amendments) requires that the suspicious transaction or activity be reported to FIU as soon as possible within 3 days of the detection of suspicion. AML/CFT Compliance Officer and/or the designated officer shall ensure that the Suspicious Transaction/Activities Reports are duly submitted to FIU, NRB in digital form as well, through goAML application. Further the Bank shall identify the attempted suspicious transactions/activities by the customer. If the customer attempted to perform the suspicious transaction/activity, then suspicious activity report shall duly be submitted to FIU within 3 days in a digital form through goAML application as per the goAML guidelines circulated by FIU. The Bank shall report suspicious transaction including attempted transaction, regardless of the amount of the transaction.

The act requires an STR to be filled by BFIs in the following situations:

- When the BFIs suspect that the asset/money is in any way related to criminal offences of money laundering and financing of terrorism or any other offences under the judicial framework.

- When the BFIs suspect that the asset/money are related to Terrorist activity, person or organization related to terrorism and/or terrorism financing, or suspect to be used in terrorist activities or by person or organization related to terrorism.

A key to recognizing suspicious transactions is to know enough about the customer to recognize that a transaction, or series of transaction, is unusual for that particular customer. So, any transaction that has a reasonable ground to arouse suspicion that the proceeds may be of illegitimate activity, may be applied in illegitimate activity or do not seem to have any rational and lawful purpose can be taken as suspicious transaction. Further, suspicion can also be roused by the behavior or identity of the customer. For such account activity/transaction or observation, the Bank shall file the Suspicious Transaction Report (STR) with FIU at the earliest as per the regulatory requirement in the prescribed format. The Bank shall not put any restriction on operation of account where an STR has been reported.

Appropriate internal record of the STR been filed will be maintained for necessary references and undertakings. Also, even if a transaction/activity is been found to be satisfactory after proper analysis, thus not requiring to raise STR, the same shall be recorded appropriately.

Some of the areas, but certainly not all, where staff should remain vigilant to possible money laundering situation are suspicious cash transactions, suspicious transaction using customers' accounts, suspicious transactions using electronic banking services, suspicious use of letter of credit, suspicious loan transactions, etc. The fact that any of the suspicion do occur in any of the areas, does not necessarily lead to the conclusion that money laundering has taken place, but they could well raise the need for further investigation on the transaction/activity.

The Bank shall extend full cooperation for any lawful request made by government agencies, and other regulatory bodies, during their investigation into money laundering without "tipping-off" the customer.

No information regarding the customer collected through CDD shall be disclosed to the unauthorized person/organization including the Bank staffs and/or family members and friends, in any means, except to the agency, organization or official(s) legally mandated to receive such information.

The detailed procedures for the reporting of suspicious transaction shall be as described in the procedural guidelines for suspicious transaction reporting framed under this policy. The copies of disclosures made to the authorities shall be retained, together with the record of all other related documents including the inquiries undertaken in regards to the submitted record. Similarly, appropriate records shall be retained regarding the non-disclosure of any internal records to the authorities to demonstrate that at the time there was insufficient justification for making such a disclosure.

The Bank shall extend full and prompt cooperation to all the legal requests to provide customer information to the authorities, necessary to assist their investigations in regards to money laundering and terrorism financing. Under no any circumstances should the customer or any other unauthorized parties are informed regarding the making of such disclosure by

the Bank, as such notifications may compromise on an existing or potential investigation by the authorities. Such act shall be punishable as per the prevailing law of land.

10 White-listing Corporate Customer

White-listing customer refers to listing of corporate customers which shall prevent the corporate customer to be red flagged in the particular AML scenarios or all the scenarios depending on the white listing done by user. The procedure of white-listing corporate customer shall be done at central level by AML/CFT department with extra caution as none of the customer categories are waived by NRB from monitoring & reporting STR.

The user at AML/CFT department shall white-list the corporate customers ensuring & analyzing the transaction conducted in the account and assuming that no such transaction shall be conducted in those accounts in future which leads to suspicion. The corporate customer (except Financial Institution & Government account, statutory institute such as Citizen Investment Trust, Employees Provident Fund, and Regulator such as NRB, SEBON and Mutual fund) shall not be white list in all scenarios types rather shall be white-list in specific scenarios type.

11 Training and Awareness

Relevant laws, regulations, policies and procedures, and other informative and educative materials shall be communicated to all the employees so that they are adequately aware of the regulatory requirements as well as the internal policies and procedures regarding the KYC and AML/CFT.

The main purpose of AML/CFT training is to ensure that the employees are aware of the risk of ML/FT faced by the Bank and how they should respond when confronted with such risks. Training will be provided on AML/CFT legislation, AML/CFT policies, procedures and controls on regular basis and all the information regarding the training shall be recorded appropriately.

The Bank shall assess the learning requirement to the BOD members due to changes in acts, policies, procedures related to AML/CFT and develop learning and development program to the Board members, executive management and major stakeholders of the Bank in coordination with internal /external expert, and other institutions like NBI, NRB and so on.

12 Recruitment/Hiring of Employees

Keeping in mind that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse banking channels, Bank will put in place necessary and adequate screening mechanism to know its Employee as an integral part of

recruitment/hiring process of its personnel. Bank shall regularly update the Employee information and their details as part of Know Your Employee (KYE).

All employees will be educated that in case, if any loss occur to a customer because of lawful submission of information to the Financial Information Unit by Bank or its staff, none of the officials of the Bank will be liable for the same. However, in case of failure to report any suspicious activities, the Bank and the related staff will be liable for punishment as per MLPA provisions.

13 Secrecy of Information

Any staffs or authorities of the Bank shall not disclose any of the reports, documents, records, details or information that have been prepared as per the requirement of AML legislation, rules, regulations, directives and guidelines, to the customer or to any other unauthorized person/agent unless the disclosure/act has been required for fulfillment of the responsibilities as per the provisions stated by the AML act, rules and directives. In case the disclosures have identified to be made against the AML legislations and this policy, the person shall be subject to disciplinary action as per the Bank's rule.

Information collected from the customers for the purpose of opening of account and/or satisfying the KYC requirements shall be treated as confidential and details thereof shall not be divulged for any purpose to the unauthorized person/entity without the express permission of the customer, unless disclosure is under the compulsion of law.

14 Retention of Record

Adequate records of identification, address verification; account opening and transactions will be retained for the prescribed period i.e. at least five years from the date of closure of accounts or execution of transaction or end of business relationship enabling to provide a clear audit trail in the event of need and investigation. Following documents and details will be retained, for the period as prescribed by law/policy after the business relationship has ended.

- Documents relating to the identification and verification of customer and related beneficial owner
- Documents relating to national and international transaction
- Documents relating to attempted transaction and business relationship
- Records relating to suspicious transaction report
- Records of employee code of conduct and trainings in regards to KYC and AML/CFT

All the documents pertaining to the prevention of Money Laundering and Combating Financing Terrorism, including the AML monitoring reports made by the Compliance Officer and the action taken as a consequence, records showing the dates of KYC and AML training and the names and acknowledgement of the staffs receiving the training shall be retained

for the period as prescribed by the law of the land. All records maintained should be available to the authorized persons promptly on request without any undue delays.

15 Employees' Code of Conduct

Staff will maintain code of conduct in regard to KYC norms/AML standards/CFT measures stating following standards in minimum.

- I will not inform/warn the customers about the suspicion of their nature of transaction
- I will not talk/disclose about ongoing investigation of suspicious transaction or about customer's activity with other employees or friends or family members.
- I will comply with the instruction given in accordance to the bank Policies by the competent authority and immediate supervisor or line manager/s

I will be liable to cooperate with the competent authorities during the process of investigation. All the employees of the Bank shall make necessary declarations and ensure full compliance with the Bank's Employees' code of ethics.

16 Roles and Responsibilities

16.1 Roles and Responsibilities of BOD

The Board of Directors shall be responsible

- To review and approve this Policy document on KYC and AML/CFT and its subsequent amendments from time to time.
- To review the reports submitted by the Compliance Officer through CEO, with respect to the Bank's compliance with legislation and other requirements contained therein and provide directions to the Bank Management as required.
- To discuss on setting up and improving mechanism to prevent customer's suspicious and abnormal transaction or money laundering based on the report submitted by the Compliance Officer, at least on quarterly basis, and make necessary arrangements to this effect.
- To review the status of implementation of Anti Money Laundering Act, Anti Money Laundering Rules, and the provisions contained in the directives, circulars and guidelines issued by regulatory bodies at least on quarterly basis and furnish the review report on the implementation of the directives to FIU on half yearly basis.

16.2 Roles and Responsibilities of CEO

The Chief Executive Officer of the Bank shall be responsible to review on quarterly basis as to whether or not the provisions of Anti-Money Laundering act, and rules, directive, order or policy formulated under such are complied with and submit a report to FIU completing the

review of the same in three months from the end of fiscal year. Further, a brief summary relating to this shall also be disclosed in the annual report of the Bank.
The Chief Executive Officer will be responsible for reviewing and approving the controlling, monitoring and reporting procedures formulated for the effective implementation of this Policy on KYC and AML/CFT.

17 Review and Amendments of the Policy

This policy shall be reviewed annually. Any amendments, if deemed necessary, to this Policy shall be approved by the BOD, except specifically mentioned in this policy. In case any confusion in the interpretation of this policy arises, the matter shall be referred to the BOD through AML Committee and the decision made therein, shall be the final and binding.

18 Power to formulate appropriate operating procedures

Appropriate guidelines, manuals and other operating procedures required for effective implementation of the provisions laid down in this Policy, will be approved by the CEO and the same shall be furnished to the BOD for information. Such procedures and supplementary guidelines shall be construed as the part of this Policy and shall be read in conjunction with the provisions contained in this Policy.

19 Consistency with Regulatory norms

This policy shall be read in conjunction with the prevailing laws of land pertaining to AML/CFT such as Asset (Money) Laundering Prevention Act 2008 (including amendments), Asset (Money) Laundering Prevention Rules, FIU Directives on KYC and AML, Unified Directives issued by NRB, Suspicious Transaction Reporting Guidelines, Threshold Transaction Reporting Guidelines, and directives, circulars, rules and regulations issued by the FIU, NRB, and other relevant act/rules/guidelines issued by other competent /regulatory authorities from time to time. If any provision contained herein this policy and procedures formulated within the scope of this policy contradict with the changing regulatory provisions in the scope of AML/CFT, the existing regulatory provisions will prevail and the provisions herein shall be deemed as void to the extent of contradiction.

20 Repeal and Saving

This policy shall supersede the previous version of Bank’s Know Your Customer and Anti Money Laundering Policy (KYC & AML Policy) 2020 approved by the BOD for implementation

on May, 2020. Any acts done, actions taken under the Policy shall be deemed to have been done and taken under this policy.

21 Revision History & Version Control

S. No.	Date of commencement	Base Version
1	November 2013	1.0
2	March 2017	2.0
3	May 2020	3.0
4	December 2021	4.0