Citizens Bank International Limited

AML/CFT Policy

Table of Contents

Abbreviations

AML/CFT:	Anti-Money Laundering and Combating Financing in Terrorism
APG:	Asia/Pacific Group on Money laundering
ALPA:	Assets (Money) Laundering Prevention Act
BAFIA:	Bank and Financial Institution Act
BFIs:	Bank and Financial Institutions
BOD:	Board of Directors
CDD:	Customer Due Diligence
COO:	Chief Operating Officer
CIAA:	Commission for Investigation of Abuse of Authority
DNBPs:	Designated Non-Financial Business and Persons
DCEO:	Deputy Chief Executive Officer
ECDD:	Enhanced Customer Due Diligence
EU:	European Union
FATF:	Financial Action Task Force
FCY:	Foreign Currency
FIU:	Financial Intelligence Unit
HPPs:	High Positioned Persons
HMT:	Her Majesty Treasury Department, UK
KYC:	Know Your Customer
ML/FT:	Money Laundering / Financing Terrorism
NF2F:	Non Face to Face Customers
NRB:	Nepal Rastra Bank
OFAC:	Office of foreign assets control
PEPs:	Politically Exposed Persons
RBA:	Risk Based Approach
RBCDD:	Risk Based Customer Due Diligence
STR:	Suspicious Transactions Report
TTR:	Threshold Transactions Reporting
UN:	United Nations

Chapter 1:
Background on AML/CFT

1 Introduction

This Policy shall be known as the "AML/CFT Policy, 2022" and shall come into force from the date of approval of the Board of Citizen's Bank International Limited. The policy has laid down appropriate framework for effective compliance to prevailing Asset (Money) Laundering Prevention Act 2064, (second amendment 2070), Assets (Money) Laundering Prevention Rules, 2073 and Directives issued by Financial Information Unit (FIU) and Nepal Rastra Bank (NRB) from time to time.

The main guiding principles of this policy are mentioned below;

a) To do business only with clients whose status and identity are fully known to the Bank.
b) To determine and record the identity, background and business of all clients.
c) To regularly monitor the relationship in order to identify unusual or suspicious activity to be able to take appropriate action, if required.

This policy is applied to all staffs, Bank functions and structures (including departments and branches) and majority owned subsidiaries of Citizen's Bank International Limited located within as well as outside Nepal. If any department, branch or business unit of the Bank is unable, to apply the standards set by this policy, such activities or transactions are not tolerated by Bank.

Money Laundering is any method to change the identity of illegally possessed money so that it appears to have originated from a legitimate source. In other words, it is a process by which "dirty money" is made to look clean. The money earned from drug trafficking, tax evasion, extortion, smuggling etc. are examples of dirty money. Money Laundering is a major concern to the governments and regulatory authorities all over the world. It has been recognized as a major social problem and crime by the governments around the world. Financial institutions are the medium for channeling the illegally or criminally earned money into the financial system. The simplest way to clean the illegally earned money is to bring-in such money to the financial system through different means such as deposits of cash, drafts, electronic transfers and other financial instruments.

Financing of Terrorism is a financial support, as the solicitation, collection or provisions of funds with the intention that they may be used to support terrorist acts or organizations. According to the International Convention for the Suppression of the Financing of Terrorism, "Involvement in any form, either directly or indirectly, unlawfully and willingly, providing or collecting funds with the intention that it could be used or in the knowledge that to be used in any act intended to cause death or serious bodily injury to a civilian not taking any active part in the hostilities in a situation of armed conflict." Funds may be collected from both legal and illicit sources. The primary goal of individuals or 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.

1.1 Risks of Money Laundering and Financing of Terrorism to the Banks

Bank is exposed to following risks through ML/FT activities.

Reputational risk: The reputation of a business is usually at the core of its success. The ability to attract good employees, customers, funding and business is dependent on reputation. Even if a business is otherwise going on the right track, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong policy helps to prevent a business from being used as a vehicle for illegal activities.

Operational risk: This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. If AML/CFT policy is poorly implemented, then operational resources are wasted. The chances of misuse of Bank's resources by criminals for illegal purposes may increase. The time and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound.

Compliance Risk: Risk of loss due to failure of compliance with key regulations governing the Bank's operations.

Legal risk: Risk of loss due to any of the above risk or combination thereof resulting into the failure to comply with the Laws and having a negative legal impact on the Bank. The specific types of negative legal impacts could arise by way of fines, confiscation of illegal proceeds, criminal liability etc.

Financial risk: Risk of loss due to any of the above risks or combination thereof resulting into the negative financial impact on the Bank.

2 Stages of Money Laundering

Usually, Money Laundering has three stages. These stages may occur separately, simultaneously or in phases overlapping one other. In all the three stages, the money obtained illegally is brought into the financial system through financial institutions.

2.1 Placement

Placement is the physical disposal of cash proceeds derived from illegal activity. It could be done through:

– Depositing of large amount of cash in numerous small amounts.

– Setting up a cash business as a cover for Banking large amount of money.

– Investing in shares and other investment products and

– Mingling of illegal cash with deposits from legitimate business e.g. car and antiques dealers.

2.2 Layering

Layering is the practice of separation of illegal money from its original source by creating complex layers of financial transactions designated to disguise the audit trail and provide anonymity. The purpose is to confuse the audit trail and break the link from the original crime. The examples are as follows:

– A Company passes money through its accounts under cover of bogus invoices, merely to generate additional transactions.

– A customer raises a loan on the security of a deposit (from illegal business) in another Bank to help break the connection with illegal funds.

– A customer incurs large credit card debts from an account.

2.3 Integration

Integration schemes place the launched funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds. It is a scheme to move illegal money into the legitimate economy so that no one would suspect its origins.

3 Regulation in Nepal

In order to combat ML/FT, laws and regulations have been formulated and implemented in various countries. In Nepal, there is stringent licensing and registration criteria of the Central Bank (Nepal Rastra Bank) for the Banks, Financial Institutions and other institutions dealing in

financial transactions. Moreover, Bank and Financial Institutions Act 2073 of Nepal have specified the qualification of Promoters, Directors and Chief Executive Officer of Financial Institutions. As per the Central Bank policy, for instance, the legitimate source of funds to invest as a promoter in financial institutions must be declared. There is an independent Financial Information Unit (FIU) established under Asset (Money) Laundering Prevention Act 2008 in Nepal Rastra Bank for collection, analysis and dissemination of information relating to the offence on AML/CFT.

Government of Nepal and Nepal Rastra Bank so far has formulated and implemented following acts, rules and directives to curb AML/CFT practices in Nepal.

a) Asset (Money) Laundering Prevention Act
b) Asset (Money) Laundering Prevention Rule
c) Unified NRB Directives No. 19
d) Unified Forex Circular No. 27

Major obligations of the Financial Institutions as defined in the said rules are as below:

a) Maintain record of the transaction and other details of the customers as prescribed by the Financial Information Unit,
b) Update customer risk profile of the existing customer as prescribed by the Financial Information Unit and maintain the record in electronic form upto 5 years and provided to FIU unit immediately in case of demanded by FIU unit.
c) Maintain a separate confidential record of the suspicious transaction signed by the concerned initiating staff, reviewing staff and AML/CFT Compliance Officer,
d) Conduct risk based customer due diligence. Enhanced due diligence for high risk customer.
e) Investigate and inquire any transaction which appears to be suspicious or transacted with the motive of asset laundering or so laundered or there are reasonable grounds for suspicion,
f) Designate a high ranking managerial level official as a AML/CFT Compliance Officer and provide the Financial Information Unit with the name, address and contact number of the AML/CFT Compliance Officer,
g) Monitoring of transactions exceptions above Threshold Transaction Limit.
h) Formulate internal responsibility and work division.
i) Conduct Risk Based customer due diligence system evaluation and its process.
j) Formulate diligence of Risk based system for Identification, maintenance and Monitoring.

k) Formulate System for diligence of unusual and Suspicious Transaction.

l) Maintenance of System for diligence of work, Completion as prescribed under point no 6 Kha of Asset (Money) Laundering Prevention Act 2064 BS Offence of Money Laundering. (Special Management regarding Blocked of Assets)

3.1 Offence of Money Laundering

Following are common offences that are frequently practiced in Nepal.

- Economically Irrational transactions.
- Use of third party in unrelated transactions.
- Cash, wire transfer and lending related suspicious activities.
- Money Laundering involving employees and agents of institutions.
- Corporate and business transactions which is economically not justified.
- Trade Based Money Laundering.
- Money Service Business related suspicious activities.
- Creation of complicated structures in Trusts where there is no legitimate economic reason.
- Use of Accountants and Lawyers as agent or intermediary without obvious reason

3.2 Prohibition on Financing of Terrorist Activities.

No one shall finance or causes to finance terrorist activities.

3.3 Offence of Financing of Terrorist Activities.

Any person commits the offence of financing of terrorist activities if that person by any means collects or provides to any person any asset with the intention that they should be used or in knowledge that they are to be used in order to carry out any act which constitutes an offence within the scope of the following conventions or any other act intended to cause death or serious bodily injuries to an individual.

3.4 BAFIA 2006 of Nepal stipulates the provisions relating to recovery from or confiscation of deposits in the following case:

In case any business or transaction is conducted by pledging as collateral or security the amount deposited with a Bank or Financial Institution, or in case amounts are deposited with a Bank or Financial Institution with misappropriated funds belonging to the government or any institution fully owned by Nepal Government, or with funds obtained by committing any action which is deemed to be an offence under current law, or with funds collected through any activity relating

to terrorism or organized crime, the concerned deposit may be confiscated or such collateral or security or misappropriated or other funds may be recovered from the deposit according to current law.

4 Objectives of the Policy

Bank has implemented this policy for identification of customers and those acting on their behalf. The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a Bank short-circuit identity procedures just because the new customer is unable to present himself for interview. The Bank should always ask itself why the customer has chosen to open an account in a foreign jurisdiction. The major objectives of the policy are:

a) To lay down a framework to be implemented by the Bank in order to safeguard it against being used for money laundering and financing of terrorism.
b) To ensure full compliance by the Bank with all applicable legal and regulatory requirements pertaining to money laundering and financing of terrorism, and
c) To provide a broad framework for formulation and implementation of various operational procedural and guidelines that is required for effective AML/CFT & KYC compliance.
d) To ensure that risk based system and process in place
e) To ensure that staff members are adequately trained in applicable AML/CFT policies and procedure.
f) To set procedures to identify ML/FT vulnerable transactions, customer identification and acceptance.
g) To prevent the opening of anonymous and fictitious accounts.

5 Fines and Penalties for non-compliance

NRB may take any or all of the following actions or fines against the Bank, its staffs and officials for failing to comply with any provisions of the Act, Rules and Directive:

Fines and penalties for individuals

Individuals involved in money laundering or terrorist activities is charged with any one or all of the below mentioned punishment

a) Individuals involved in Money Laundering is charged twice amount fine of the laundered amount and 2 to 10 years of imprisonment.
b) Individuals who involves in master planning of Money Laundering are charged with full punishment as stated in above and individual involved in other act are charged with half of punishment as stated in above.
c) Individual involved in financing in terrorist activities are charged with five times of laundered amount, if laundered amount is disclosed else if not disclosed fine amount could be maximum of Rs. 1 Crore and also 3 to 20 years of imprisonment depending the fault act.
d) Individuals using legal power for money laundering and financing in terrorist activities are charged with punishment as stated in above.
e) In case of individuals, employees are not identified then the immediate supervisor of that period shall attract legal and disciplinary action.
f) Employees found involving in money laundering and financing in terrorist activities shall attract 10% additional punishment with prevailing all above punishment.
g) Employees tipping off and leaking the secrecy are liable to one month to 3 months of imprisonment or maximum Rs. 1 lakh or both punishments could be charged.

Fines and penalties for Legal Entities

Legal entities involved in money laundering or terrorist activities is charged with any one or all of the below mentioned punishment

a) Charged with five times of laundered amount.
b) Prohibit to purchase or production or use service.
c) Reimburse the amount of loss or damage
d) Termination of License or Deregistration of Legal entity.
e) Legal entities using legal power for money laundering and financing in terrorist activities are charged with punishment as stated as for individuals.

Fines and penalties for non-compliance to Bank

Bank's failure to mitigate money laundering or financing terrorism risk maybe charged with any one or all of the below mentioned punishment.

a) Fines and Penalties as per Unified Directive 19
b) Fines and Penalties as per Unified Forex Circular 27

6 Bank's Approach to AML/CFT

There is strategic orientation of Bank on restraining risks related to money laundering and terrorist financing. This policy has set expectations, standards and behaviors on AML/CFT. The Bank's approach to AML/CFT is designed to help the business meet their responsibilities in relation to the prevention of money laundering and financing of terrorism. These standards are primarily based on the relevant laws / regulations / statutory guidelines and the best practices on prevention of ML/FT. As the Bank is committed to prevent from money laundering and financing of terrorism, the Bank will:

a) Establish clear lines of internal accountability, responsibility and reporting.
b) Document, implement and maintain Policies, Standard Operating Procedures which interpret/ implement this policy and set standards for each business in line with the law, regulations and regulatory guidelines.
c) To implement automated AML solutions across its network for effective KYC management, risk assessment, transaction monitoring etc.
d) Report any transaction where, based on explanations offered by the customer or other information, reasonable grounds exist to suspect that the funds may not source from a legitimate source or are to be used for an illegal activity or to be used for financing of terrorism or if customer / applicant / beneficiary refuses or fails to submit required information/ documents.
e) Conduct periodic and regular trainings on money laundering and financing of terrorism in order to raise awareness among employees on ML/FT methods to recognize suspicious transactions, the regulatory requirements and the procedures and controls adopted by the Bank to control / prevent money laundering and financing of terrorism and other relevant matters.
f) Support regulatory body and law enforcement agencies in their efforts to combat the use of the financial system for the laundering of the proceeds of crime or the movement of funds for criminal purposes.
g) Take all reasonable steps to verify the identity of customers, including the beneficial owners and established procedures to retain adequate records.
h) Exercise due diligence in establishing correspondent relationships with local / foreign Banks.

i) Install adequate system of checks and internal control to prevent the money laundering and the financing of terrorism, and

j) Treat the issues pertaining to the money laundering and financing of terrorism as "Zero Tolerance Issues" and take action as a high priority issue.

6.1 Three lines of defense

For the effective assessment, understanding, management and mitigation of ML/FT risks, Bank shall adopt three line of defense. Identification and analysis of ML/FT risks and effective implementation of policies and procedures to encounter the identified risk is the feature of effective and sound risk management. These lines of defense shall act as safeguard to the Bank during the adversities and shall be liable for effective risk management.

First line of defense: Business units and departments shall function as a first line of defense to prevent ML/FT risks. Business shall promote AML/CFT principles as well as business. Persons involved in business functions must ensure that appropriate controls are in place and operating effectively. Business units shall make an appropriate risk assessment before introducing any product or service and implement required mitigations. It shall be the responsibility of AML/CFT Department to assist business units/departments in this process.

Second line of defense: AML/CFT Department shall function as a second line of defense to prevent ML/FT risks in the Bank. The AML/CFT Department shall monitor overall legal, regulatory and internal compliance of policies, procedures and guidelines. It shall also provide businesses with regulatory compliance expertise and guidance, set standards and trainings for businesses to manage and oversee ML/FT risks.

Third line of defense: This shall be performed by internal audit. The internal audit shall review the activities of the first two lines of defense with the purpose to ensure that legislation, regulations and internal policies are processed effectively.

6.2 Sanction Policy

The Bank's policy has defined minimum standards in which the Bank must comply with the sanctions laws and regulations of the United Nations (UN), the European Union (EU), the United Kingdom (HMT) and the United States (OFAC), as well as all applicable sanctions laws and

regulations in the jurisdictions during establishing any kind of relationship. The sanction screening is defined by "Sanction Screening Policy" framed under this policy.

6.3 Risk Assessment of Bank

The Risk Assessment of the Bank is process of identification of money laundering and financing terrorism risk through various components of the Bank and determining the risk mitigates by use of proper controls. The purpose of Risk Assessment is to strengthen internal control system of the Bank through the development of ML/FT risk mitigation strategies. It identifies the Bank's risk exposure by assessing and defining risk grading of each customer, product, services, delivery channels and geographic location of the Bank by ways of specific format for recording of each data/information required for effective risk assessment. It determines risk mitigates by use of proper controls.

The Risk Assessment procedure include identification of gaps or opportunities for improvement in AML policies and procedures is also assessed and it also help in making decisions about risk appetite and implementation of control efforts and effective allocation of resources and technology to high risk areas. It is a continuous process, further actions to be carried out.

- Prepare report of risk assessment on basis of risk factors such as customers, products/services, transactions, country, geographic areas and delivery channel.
- Analyze with varying degrees of impact and levels of risk and type of mitigation to be applied.
- Conduct risk assessment on annual basis and provide risk assessment information to NRB.

The Bank shall adopt Risk Based Approach (RBA) in managing its ML/FT risks and assess potential ML/FT risks and implement measures and controls commensurate with the identified risk. The Bank shall strengthen, make priorities and perform its activities to manage higher risks first and ensure that greatest risks receive the highest attention. RBA shall be adopted in all activities that are performed to prevent ML/FT risks in the Bank.

6.4 Cooperation to regulatory body and law enforcement agencies

Co-operate with any lawful request for information made by regulatory body / enforcement agencies to assist in their investigations into money laundering and financing of terrorism. Support regulatory body / enforcement agencies in their efforts to combat the use of the financial system for the laundering of the proceeds of crime or the movement of funds for criminal

purposes. Bank shall ensure that all the instructions and letters received from various enforcement agencies shall be enacted upon the stipulated time.

6.5 Tipping Off

The Bank or any of its staff (including board members) shall not disclose to its customer or to any other person that a following report, document, record, notice or information concerning suspected money laundering or terrorist financing or predicate offence has been initiated or is being submitted to FIU and/or any other enforcement authorities and their officers:

a) Report of suspicious or threshold transaction
b) Order received from FIU or any other enforcement authorities for conducting ongoing monitoring of any customer.
c) Any document, record or information provided to the FIU and other investigating authorities
d) Disclosing name and any other detail of Bank staff/s providing report, document or information to concerned authorities

As per provision of ALPA, information shall not be disclosed even in judicial proceedings that discloses or may disclose the introduction of official or staff

ALPA has allowed NRB to fine up to one million rupees fine to the Bank if tipping off is done. Similarly, the Bank is to take departmental action to its staff as per Employee bylaws.

6.6 Code of conduct

As a responsible staff of the Bank, every staff of the Bank shall adhere following code of conduct relating to prevention of money laundering and combating financing terrorism:

a) No staff or official of the Bank is supposed to have violated the professional or financial norms prescribed under other prevailing laws, if such act has been carried out in the course of discharging duties under the Asset (Money) Laundering Prevention Act up to the level of performance mandated under the Act.
b) No any staff of the Bank (including board members) shall, by any means, be involved in money laundering or terrorist financing directly or indirectly, in part or in whole, unlawfully and willingly.
c) No any staff of the Bank (including board members) shall, by any means, support to money laundering or terrorist financing directly or indirectly, in part or in whole, unlawfully and willingly.

d) No any staff of the Bank (including board members) shall inform / share / talk / disclose / warn, by any means, to any unauthorized persons about the Bank's policies and procedures relating ML/FT risk management.

e) No any staff of the Bank (including board members) shall inform/share/talk/disclose/warn, by any means, to any unauthorized persons about Bank's consideration as suspicious or any investigation initiated by Bank or other competent authorities regarding any of its customers or other parties.

f) No any staffs of the Bank (including board members) shall tip off or inform/ share / disclose / warn, by any means, to any of the Bank's customer.

g) Concerned staff shall provide access to offices or furnish information requested by authorized persons of the Bank entrusted with responsibility of legal and regulatory compliances.

h) Concerned staffs shall extend full cooperation to the legal and regulating bodies during their investigation in relation to ML/FT activities.

i) No staff (including board members) shall provide customer or any third party, at the customers' request, with incomplete or otherwise misleading documents or information in connection with the customer's accounts and transactions.

6.7 Whistle Blowing

The speaking up mechanism instigated in the Bank such that any staff member who suspects that the Bank's code of conduct, prudent practice and ethical standard is being/has been compromised contemplating or facilitating any act of ML/FT are allowed to escalate the case to senior management. Furthermore, staffs can speak-up if they suspect any actual, planned or potential wrong doing that include bribery, corruption, fraudulent practices and abuse of authority or resources of the Bank.

No criminal, civil, disciplinary or administrative action or sanction shall be taken against the Bank or any of their official or staff who in good faith submit reports or provide report, document, information, notice or records in accordance with the provisions of ALPA, rules and directives as a breach of secrecy provision under prevailing laws or contractual, administrative or regulatory liability. The management shall provide adequate safeguards against victimization of speaking up including the anonymity of the speaking up.

6.8 Employee Training programs

Compliance with Statutory and regulatory requirement: The Bank is responsible to fully complied the entire statutory and regulatory requirement relating with training and awareness of the employees.

Risk Based Approach: The Bank shall adopt a risk based approach while conducting training programs. The Bank shall aim, strengthen, prioritize, and conduct trainings in line with the result of Bank's risk assessment as well as emerging ML/FT risks identified by the Bank.

Education and Training programs: The Bank shall conduct educational and training programs relating to ML/FT risks and their management as its regular activity. It shall be the Bank's policy to provide basic awareness training to staffs, senior executives and shareholders holding more than 2% shares. Such programs may include seminars, workshops, discussions, trainings etc. The Bank shall conduct such programs on a regular basis. All education and training programs shall be conducted as per the guideline framed under this policy.

Adequacy and effectiveness: The AML/CFT Compliance Officer shall determine the adequacy and effectiveness of the programs.

Record Retention: The Bank shall maintain the record of all education and training programs conducted by the Bank. Such record is kept in a way that it is capable of disclosing name, date, major issues discussed/covered, participants, etc.

6.9 Anti-Bribery and Corruption Policy

The ABC Policy applies to all the stakeholders of the Bank. In addition, relevant employees will be required to attend training to support the guidance in this policy.

The Bank does not condone or consent to any associated person to corruptly soliciting, receiving or agreeing to receive any gratification whether for him/herself or for any other person or corruptly giving, agreeing to give, promising or offering to any person any gratification whether for the benefit of him/herself or of another person, as an inducement to or reward for obtaining or retaining business for the Bank, any advantage in the conduct of business for or affairs of the Bank or for any other person, or doing or forbearing to do anything in respect of any matter or transaction in the conduct of business or affairs of the Bank.

All forms of bribery and corruption are prohibited and Bank will not tolerate any act of bribery or corruption. Any breach of this policy or local law could result in disciplinary actions and ultimately could result in dismissal. It shall be the responsibility of all employees to know, understand and comply with this provision.

This provision sets out a single standard that all employees must comply with, Failure to comply with this provision, may lead to disciplinary action and criminal liability for the individual involved.

Risk Based Approach to Mitigation

To help ensure that business is conducted without bribery and corruption, Bank is committed to

- Conducting regular evaluation of Bank's business policies to identify, mitigate and control potential bribery and corruption risks.
- Senior Management has the collective responsibility. Management staffs at all levels are responsible for ensuring those reporting to them are made aware of and understand this provision and are given adequate and regular training on it.
- Rotation of employees to different jobs on a regular basis.
- The segregation of duties of employees.
- Zero - tolerance approach to bribery and corruption.
- Conducting thorough background checks on new employees.
- Training should be done regularly, and should be documented. A training program should include examples of corruption and bribery, as well as red flags.
- Regular Audits. Any red flags that are uncovered during an audit should be dealt with using the Bank's compliance program.
- A declaration form covering the provision of Anti Bribery and Corruption to be included in every tender document of the Bank.

Chapter 2:

Risk Based Customer Due Diligence

1 Policy

Adherence to RBCDD policy is essential for the safety and ethical standards of the Bank's operation. The Bank is committed to preventing itself from being used for ML/FT purposes. The Bank is always ready to extend cooperation to regulators, prosecutors, and other Government authorities to stop its Banking channel from being used for illicit financial activities. CDD is more than Know Your Customer (KYC). CDD means:

a) Identifying& verifying the customer's identity including any person purporting to act on behalf of the customer from independent and reliable source.
b) Identifying and verifying beneficial ownership and control
c) Establishing intended purpose, nature of the business relationships.
d) Conducting ongoing due diligence, scrutiny of relationships, transactions & keep records up to-date

1.1 RBCDD policy in brief is as follows:

a) No opening of account or conducting transaction on anonymity or fictitious name or of any person / organization listed as terrorist in the website of Ministry for Foreign Affairs of Nepal, OFAC (Office of foreign assets control), and any website suggested by FIU and management from time to time.
b) Should obtain approval from Chief Operating Officer (COO) or Head Operations (in case of absence of COO) for opening account of High Risk Customers.
c) Confirmation of actual information of customer and beneficiary by documentation verification.
   - In establishing business relation
   - In carrying out transactions above threshold
   - In carrying our wire transfer
   - In suspected transactions/activity
d) Certify KYC independently with trustworthy source and maintain such documents.

e) Must obtain proper identification documents of the customers/originator& input information in CDD form and verify the authenticity in following situations, wherever applicable.
   - Before establishing business relations with the customer.
   - Customers conducting series of transactions below the threshold on regular basis.
   - Transactions through wire /swift / TT.
   - There is a suspicion of money laundering or terrorist financing.
   - If there is doubt on previously submitted identification document.
   - any time of transaction in relation to the high risked and politically exposed person,
   - In any other situations as prescribed by the Regulator.

f) Cash deposits more than Rs 1,000,000/- in an account
   - Obtain documents evidencing source of the amount or obtain declaration from customer that the money is received from sources other than terrorism, drug smuggling, human trafficking, and organized crime.
   - Conduct Enhanced CDD if suspicion arises.

g) Special attention should be given to all complex, unusual large transactions, or unusual patterns of transactions that have no visible economic or lawful purpose.

h) Keep such findings available for examination by the FIU, auditors, and any other competent authorities, for a minimum of five years.

i) Obtain declaration of loan facility from multiple Banking when providing credit facilities to individuals, firms, companies or corporations.

j) Obtain Identification document the customer for each transaction amounted to Rs one lakh or equals or above foreign currency as prescribed under rule 3 of Assets (Money) laundering Prevention Rule 2073.

k) If any person other than the account holder wants to deposit cash in the account, then the branch must obtain documents and details furnishing the identity of the client along with purpose of deposit from the depositor for cash deposit above NPR 1 Lakh.

l) Only KYC of signatories mandatorily to be obtained during Identification and Verification of following institutions,
   - Nepal Government and Offices
   - Entity established under Special Act
   - Government Holding Organizations

- BFI licensed by NRB
- Office of UNO & International Organization
- Foreign Embassies

m) Application of CDD requirements to existing customers on the basis of risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

n) Perform enhanced due diligence where the ML/TF risks are higher.

o) Application of simplified account opening measures where lower risks have been identified. The simplified measures should be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.

p) Where unable to comply with relevant CDD measures:
   - Required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship.
   - Required to consider making a suspicious transaction report (STR) in relation to the customer.

q) Adopting risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.

r) In cases of suspicion of money laundering or terrorist financing, performing the CDD of such customer will lead to tip-off, so CDD of such customers should not be conducted and instead should be required to file an STR.

s) Obtaining additional information regarding high volume of annual income for non-income generating occupation during account opening like student, housewife and minor.

2 Process

Branch Managers / Customer Relationship Officers or other designated staff are responsible for interviewing the prospective customer and obtain sufficient information on the reputation of the client, legitimacy of the business and nature and source of activity expected in the account. Operation in Charge or designated staff in Branches shall verify and retain copies of required documents of any individual or any legal entity for future reference.

Business relationship should never be established until the identity of the potential customer is satisfactorily established. If a potential customer refuses to provide the requested information, the relationship should not be established. Likewise, if the requested follow-up information is not forthcoming, any relationship already begun should be terminated. Branch Managers/ Customer Relationship Officers or designated staff should not approve/recommend new accounts unless proper identity of the account holder is established as per the parameters set out in this policy.

In brief, following procedures should be observed on account of any customer / potential customer of the Bank.

- Identification of customer and beneficiary / beneficial owner.
- Collect information of customer and beneficiary or beneficial owner.
- Assignment of risk profile.
- Decision on accepting new customers.
- Update information of customer and beneficiary or beneficial owner.
- Monitoring of customer transactions.
- ECDD or CDD as per the risk.

3 Courteous Conduct

The purpose of AML/CFT Policy is to establish the identity of the prospective customer and to verify the source of large funds. Accordingly, the KYC interview should be conducted in a very polite manner and it should not amount to a detective investigation.

It must be recognized that trade and commerce in Nepal is still largely cash based and undocumented. Every cash transaction or inability to provide supporting documents should not automatically lead to suspicion. In case of doubt, the advice of AML/CFT Compliance Officer should be obtained before making a decision.

Chapter 3:

Customer Acceptance Policy

1 Customer Identification

It is essential to establish the true identity of the customers and be assured that the customers are not involved in any kind of money laundering and terrorist activities. Some of the key information that the Bank requires to collect includes;

a) Information regarding the family member's
b) Full customer identification evidence
c) The reason for the relationship recorded with sufficient detail to provide an understanding of the purpose of the account and the nature of the customer's business or employment.
d) An indication of the anticipated volume and type of activity to be conducted through account.
e) Bank's understanding of the source of funds routed through the account
f) Recording of the underlying source of wealth in case of High Net Worth accounts.
g) One on whose behalf the account is maintained i.e. beneficial owner
h) Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, and Solicitors etc. as permitted under the law.

   Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Bank. For instance,

   - Person involved in transaction through wire transfer.
   - Person who transacts above Rs 1 million in a single transaction or series of transactions through wire transfer or similar mechanism in a day.
   - Person who exchanges FCY equivalent to above Rs 5 lakhs in single transaction or series of transactions in a day.

The Bank shall take all reasonable steps to verify the identity of customers, including the beneficial owners of corporate entities and individuals as well, and the principles behind customers who are acting as agents. The Bank will take all reasonable steps to ensure that "Customer Due Diligence" information is collected and kept up-to-date and that identification information is updated when changes come to the Bank's notice regarding the parties involved in a relationship. In account opening through online account opening system, Bank can be sure and

possibility on confirming customer identification and their geolocation through electronic medium.

The Bank has established procedures to retain adequate records of identification, account opening and transactions, account opening records and transaction records shall be retained for minimum five years after a relationship has ended. Records relating to internal and external suspicious transactions reports should also be retained for a minimum of five years.

2 Beneficial Owners

Beneficial Owner means a natural person who, directly or indirectly, owns or controls or directs or influences a customer, an account, or the person on whose behalf a transaction is conducted, or exercises effective control over a legal person or legal arrangement or remains as an ultimate beneficiary or owner of such activities.

a) Maintain mechanism for Identification of real Owner, transaction monitoring, inquiry from other Customers, publicly available information, information obtained from regulatory authority & Business database.
b) Review the completely filled up KYC form and CDD form. If any customer having beneficial owner, the Bank should identify beneficial owner / Obtaining authority letter for their agents and verify necessary information from different sources.
c) Maintain the details of customers/beneficial owner in an electronic means whose details can be generated and reported any time.
d) Obtain the necessary documents of customers from other appropriate and reliable medium except in cases where the customer presents himself physically.
e) Branches/Departments should gather sufficient information from a new customer and check for publicly available information (i.e. analysis of social sites, Database of involvement in Business) in order to establish whether or not the customer is among a HPP.
f) Only the documents submitted along with KYC forms or CDD obtained from domestic or international inter-mediatory can be relied in following conditions.
   - Listed public limited companies in Nepal
   - Listed companies of foreign countries that have complied/implemented the international standards on sound and effective AML/CFT Policies domestically or internationally.

- Not falling on FATF list of high risk jurisdictions subject to a call for action and jurisdictions under increased monitoring, list of terrorist maintained by home ministry, UN, OFAC, EU and HMT Sanctioned List.
- Upon Bank's own risk and confirmation.

g) While verifying KYC / CDD form of other legal persons, obtain details of each ultimate controller, natural persons or owner of limited liability companies or firms:
   - of persons holding 10% or more shares or voting power.
   - Person controlling the legal entity or exercising controlling rights over such entity. For e.g. BOD members, trusty and beneficiary of a trust.
   - of managerial people
   - (in case of Guthi)- BOD member, trusty and beneficiary of trust
   - Chairman and Managing Director for those entities whose shareholding is not defined.

h) Determining the indirect interest/ownership in shares (*while calculating 10% above*):
   - Proportionate share holding, partnership or beneficiary of a company in another company, limited liability partnership or corporations and trust (Guthi)
   - Of person/group of persons/members of single family controlling the entity (family members include Spouse, son, daughter, parents (including step mother), grandparents, brother, sister and grandchild)

i) Adoption of additional measures such as verification in website, etc for any customer from countries deficient or non-applying or inadequately applying AML/CFT measures.

j) In reference with NRB Directive 19.2 (7), there is no need to obtain the ultimate beneficial owner of below mentioned entities;
   - Government Organizations
   - Bank and Financial Institutions
   - Insurance Companies
   - Subsidiary entities of United Nations
   - Embassy and Consulate of foreign nations

2.1 The importance of identification of beneficial owner

The ultimate beneficial of customer should be identified as there are chances of misuse for illicit purposes, including money laundering, financing terrorism and other unlawful activities. This is because, for criminals trying to circumvent AML/CFT measures, corporate entities provide an attractive avenue to disguise the ownership and hide the illicit origin. In general, the lack of adequate, accurate and timely beneficial ownership information facilitates ML/TF by disguising:

a) The identity of known or suspected criminals or PEPs or HPPs.
b) The true purpose of an account or property held by a customer.
c) The source or use of funds or property associated with a customer.

2.2 Ways in which beneficial ownership information can be concealed

Beneficial ownership information can be concealed through various ways, including but not limited to;

a) Use of shell companies especially in cases where there is foreign ownership, which is spread across jurisdictions.
b) Complex ownership and control structures involving many layers of ownership, sometimes in the name of other legal persons and sometimes using a chain of ownership that is spread across several jurisdictions.
c) Use of close associates or relatives by PEPs and HPPs to conduct their transactions.
d) Use of power of attorney of individual account by other than intermediate family members.
e) Use of legal persons as directors.
f) Trust and other legal arrangements, which enable a separation of legal ownership and beneficial ownership of assets.

3 Politically Exposed Person (PEP) and High Position Persons (HPP)

The Bank shall establish a risk management system to identify whether a customer, person seeking to be customer or a beneficial owner of a customer or transaction is a politically exposed person (including foreign and domestic). The inclusive list of Political Exposed Persons, High Profile Persons and close associates is included in AML/CFT Procedures framed under this policy. It shall adopt the following additional measures if it finds the customer or beneficial owner is PEP / HPP:

a) to obtain approval from Chief Operating Officer (COO)or Head Central Operation (in case of absence of COO) while establishing a business relationship,

b) If existing customer is identified as PEPs or HPP then account should be upgraded as high risk account.
c) to take all reasonable measures to identify the source of amount/fund and property of such customer or beneficial owner,
d) to obtain information and identification documents of family members and close associates on the basis of risk or on-need basis.
e) to conduct ongoing monitoring of such customer and the business relationship,
f) to apply enhanced customer due diligence (ECDD) measures

4 High Net Worth Customers (HNW)

There is no exhaustive definition of high net worth customers as such. As per the provision mentioned in Clause 6 of Unified NRB directives 19, "High Net worth" parameters for this purpose shall be determined by the Bank itself. In line with the above provision, the Bank shall identify the HNW, verify the identity of the HNW taking reasonable measures to. Identification of HNW shall be performed as per the AML/CFT Procedures framed under this policy.

5 Non Face to Face Customers (NF2F)

Non face-to-face customers (NF2F) are those who on boarded the service provided through without face to face contact and interview i.e. via electronic medium. The nature of NF2F customers and transactions are as follows;

a) Account opening through online account opening system
b) Cross border Correspondent Banking
c) Fund transfer through remittance, swift or wire transfer
d) Transaction through Internet Banking, automatic teller machine, Mobile Banking, credit card
e) Transaction through instruction / request by internet

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 wish to avoid face-to-face contact. 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 has paid special attention to any money laundering patterns that may arise from NF2F customers and transactions that favor anonymity and be used to facilitate money laundering, and Bank must take appropriate measures to treat with such patterns. The Bank has restrained online account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures. Initial application forms could be completed on-line and then followed up with appropriate identification checks.

This policy addresses non face-to-face customers and their transactions which have an inherent ML/FT risk. Identification of NF2F customer shall be performed as per the AML/CFT Procedure framed under this policy.

6 Designated Non-Financial Business& Professionals (DNFBPs)

The entities or persons that have similar potential to financial institutions to be used for money laundering are categorized under this group. Designated Non-Financial Business Professions (DNFBP) are considered attractive channels for money laundering, financial crime and terrorist financing operations. Increased sophistication in money laundering techniques, such as the use of legal persons to disguise the true ownership and control of illegal proceeds, have brought these businesses under financial scrutiny. The list of entities and person under this group is as follows;

a) Real Estate Agents
b) Dealers in vehicles
c) Money Service Business
d) Casinos
e) Jewelers and Bullions
f) Auditors and Accountants
g) Antique Dealers
h) Import and Export Trade Business
i) Lawyers and Notaries and other independent legal professionals
j) Trust
k) Proprietors of DNFBP entity

7 Cash Intensive Business

Cash-intensive businesses are those which experience a high volume of cash flows. Cash intensive businesses and entities cover various industry sectors. Most of these businesses conduct legitimate business however, some aspects of these businesses may be vulnerable to money laundering or terrorist financing as cash intensive business may potentially be used as vehicle for money laundering and the financing of terrorism. Owning a cash-intensive business is often a goal for money launderers; as these provide an opportunity to integrate large volumes of cash into the financial system. Disguising proceeds from illegal activities or crimes as trading income of a business is one method to achieve the integration.

Criminals and money launderers may use cash intensive businesses for money laundering and financing of terrorism by using cash intensive business to:

- Provide a medium to launder large amounts of cash and reinvest the cash proceeds of crime in generating income,
- Mix the legal and illegal income,
- Invest the proceeds of cash intensive business in terrorist activities (often in small amounts), without traceability.

Examples of mentioned in the Policy on Handling Cash Intensive Business framed under this policy.

8 Customer Acceptance

The following customer acceptance indicating the criteria for acceptance of customers shall be followed in the Bank. The Bank will take all reasonable steps to verify the identity of customers, including the beneficial owners of corporate entities, and the principals behind customers who are acting as agents. The Bank shall accept customer strictly in accordance with the said policy:

a) The Bank will not accept any person/entities as its customer if the customer and beneficial owner of the customer cannot be identified verified and thus Bank is unable to have customer's risk profiling as required by the Act, Rules and Directive
b) No account should be opened in anonymous or fictitious name. Branch will collect accurate & full name of clients and preserve documents in conformity with it. Branch will prepare proper KYC of the clients.

c) Clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered and social status. Categorization customers into different risk grades.

d) Identify the person who ultimately controls a natural person or legal entity. This identification always will be a highly context-dependent, de-facto judgment; beneficial ownership cannot be reduced to a legal definition.

e) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practices of financial service as there could be occasions when an account is operated by a mandate holder.

f) Identify the customer falling under Politically Exposed Persons, High Positioned Persons, High Net Worth, Designated Non-Financial Business Group, belonging to highly corrupted countries or originated from the countries known to be high risk, conducting non face to face transactions.

g) Checking in sanction screening before establishing relationship with customer to ensure that;
   - Individuals and entities do not fall in sanction list
   - Entities are not shell Bank or companies
   - Political Exposed Persons
   - Link to highly corrupt or high risk countries

h) The status of a customer may change as relation with a customer progresses. The transaction pattern, volume of a customer's account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measures to monitor customer's activities throughout the business relation.

i) The customer is accepted only after complete KYC information or details and document required for account opening is provided by customer.

8 Prohibited customers and transactions

(a) Establish or maintain dummy accounts, anonymous accounts, or accounts in fictitious names or transact in such accounts or cause to do so;

(b) Maintain relationship with shell Banks or other Banks which deals with shell Bank or shell entities;

(c) Establish an account or continue business relationship or conduct transaction with the customer who cannot provide documents, information and details required for the customer

identification and verification as required by law and regulation. However, in case customer submits valid reason for inability of presenting some document or information and Bank become satisfied with the reason, relationship can be established and transaction can be done with maintaining record of the information of non-existence of document/information;

(d) Customers who provide conflicting Documents, information and details;

(e) Maintain relationship with the Banks operating in offshore jurisdictions;

(f) Maintain relationship with persons and entities sanctioned by major sanction authorities such as United Nations, Office of Foreign Assets Control- United States, Her Majesty's Treasury- United Kingdom;

(g) Payment orders with an inaccurate representation of the person placing the order;

(h) Acceptance of payment remittances from other Banks without indication of the name or account number of the beneficiary;

(i) Use of accounts maintained by financial institutions for technical reasons, such as sundries accounts or transit account, or employees' accounts to filter or conceal customer transactions;

(j) Maintaining accounts under pseudonyms that are not readily identifiable;

(k) Opening Accounts without name or with notional name;

(l) Acceptances and documentation of collateral that do not corroborate with the actual economic situation or documentation of fictitious collateral for credit granted on trust;

(m) Payable through Accounts;

(n) Providing Downstream Correspondent Banking;

(o) Maintain relationship with shell entities or other entities or individuals which deal with shell Bank or shell entities.

Chapter 4:

Assignment of Risk Profile

1 Establishment of Customer Risk Profile

Risk profile shall be evaluated considering influencing factors such as geographical, occupational, professional and sectoral, customer type, product or service type, nature of transaction, and distribution medium, etc. Risk identified by the government and reputed regulatory International Organization shall also be considered.

Generally, following steps are involved for determining the risk profile of any customer: -

a) Get the KYC Form completely filled up and verified by Branch Manager.

b) Scrutinize customer and information provided during regular due diligence. Care should be given for documents management, records of objective/ amount/ source/ transaction profile/ type or nature. And special watch to unusual, large, complex transactions, etc.

c) Formulate the process and procedure to identify the risk based customers (high, medium, and low) and the process, procedure to identify, update and gather the information of customers based upon the profile of respective customer, their transaction place and the type of service they avail.

d) All customer accounts and relationships shall be assigned a specific customer risk grade. The Bank shall adopt three levels of KYC risk grading system in the Bank. They are:
   - High Risk Customer
   - Medium Risk Customer
   - Low Risk Customer

e) Assign, in core Banking system, the risk category of the account.

j) The Bank shall follow risk based approach in conducting customer's due diligence as shown below:
   - High Risk Customers - Enhanced Customer Due Diligence (ECDD)
   - Medium Risk Customers - Customer Due Diligence (CDD)
   - Low Risk Customers - Customer Due Diligence (on need basis when suspicious activities observed)

f) Obtain Multiple Banking Declaration from the customer while availing credit facilities to the customers.
g) Collect documents as per assigned risks including of controller or beneficiary.
h) Ascertain objective of relation with Banks.
i) Obtain detail of source of income in case of high risk customer.

1.1High Risk Customers

Following customers are generally at high risk that may involve in investment or financing to AML & CFT purposes: -

a) High Positioned Persons (HPPs)
b) Politically Exposed Persons (PEPs)
c) Non Face to Face Customers (NF2F)
d) High Net Worth Customers (HNW)
e) Designated Non-Financial Business &Professionals (DNFBPs)
f) Business relationships and transactions with natural and legal persons (including financial institutions) from countries which is grey list category as per FATF.
g) Persons whose transactions suggest that they might be intended for an illegal purpose, or the economic purpose of which is not discernible.
h) Cash intensive Business and its related persons like petrol pumps are categorized as high risk status as per their nature of business. Restaurants, party palaces, hotel, lodge, resorts, retail stores, supermarkets, parking management entity, nightclubs, discos and travel & tours are categorized as high-risk category as per their transaction volume as per point 3.5 of chapter 3 of AML/CFT Procedure of the Bank.
i) Possible to use corporate vehicle for private property.
j) Complex corporate structure with no clear objective.
k) Massive or unduly intended cash transactions without reasons.
l) Accounts opened by professional intermediaries (the client account opened by a professional intermediary on behalf of a single client or 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.)
m) Customers who conducts transaction from electronic medium by systematically important and unusually suspicious.

n) Customers being convicted in any offence or involving moral turpitude from a court.
o) Account blocked by Nepal Rastra Bank or other enforcement agencies. However, in case of block release, the customer should be kept for high for 2 years from release date after then it could be risk downgraded after annual review.

Branch should conduct ECDD for high risk customers and obtain approval from Chief Operation Officer (COO) or Head Central Operation (in case of absence of COO) for opening such high risk customers. ECDD should justify Source of Fund and limit of the Transactions. Photocopy of Citizenship of immediate family members (in Case of minor-identification document) must be obtained of those Customers whose ECDD has to be conducted.

1.2Low Risk Customer

These are the type of customers whose identity and source of income clearly disclosed and the transactions in the accounts do not raise any suspicion. Normally, following customers may be categorized in low risk.

a) Banks/FIs regulated by NRB or of foreign countries that strictly implementing AML / CFT Policies.
b) Listed public companies in NEPSE and stock exchange of other countries implementing AML/CFT policies.
c) Salaried employees whose salary structure is well defined.
d) People belonging to lower economic strata of the society whose accounts show small balances and low turnover.
e) NGOs promoted by United Nations or its agencies may be classified as Low Risk customers.
f) Institutions conducting programs related to any productions or social service for social and economic benefit of Nepalese Citizens. However, NRB approval is required for conducting programs crossing 3 months.

1.3 Medium Risk Customers

a) The individuals and entities conducting annual transaction as per para 3.5 of chapter 3 of AML Procedure of the Bank.
b) Business relationships and transactions with natural and legal persons (including financial institutions) from countries which is categorized as tax haven and having highly secretive banking.

c) Individuals or entities who have FCY accounts
d) Stock Broker Entities
e) Investment Entities
f) Merchant Banks
g) Cooperatives
h) Non-Government Organizations
i) International Non-Government Organizations
j) Non-Profit Organizations
k) Societies
l) Welfare and Charities accounts
m) Fund
n) Customers not falling either on high risk or low risk are also to be classified as Medium Risk Customers.

2 Periodic review of Customer Due Diligence

The Bank shall view CDD as an ongoing process and therefore, CDD information of the customers shall be regularly updated. The frequency of reviews and update shall be determined by the level of risk associated with the relationship. Any information on change in the ownership and/or change in persons controlling a relationship or any other worthy / requiring information shall be taken as a trigger to update CDD information. While updating KYC information and Documents, only changed information / documents are to be obtained instead of whole documents.

Further, in line with the clause no 8.2 of NRB Unified Directive no 19 related KYC information and documents including ECDD of customer including beneficial owners shall be reviewed and updated of KYC information and details to be immediately updated upon trigger of below events:

a) At least on annual basis for high risk customers
b) Within three years for medium risk customers
c) As on need basis for low risk customers
d) Any deviations in the declared transactions
e) Where Bank's feel suspicious on any information or details provided by the customers.

Chapter 5:

Monitoring of Customers

On-going monitoring (On-going due diligence) is an essential aspect of effective KYC procedures. Banks can only effectively control and reduce the risk if we have an understanding of normal and reasonable account activity of the customers so that we have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, we are likely to fail in our duty to report suspicious transactions to the appropriate authorities in cases where we are required to do so. The extent of the monitoring needs to be risk-sensitive. Particular attention should be paid to transactions that exceed the threshold limits. Certain types of transactions should alert Banks to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. Examples of suspicious activities, annexed with this report, can be very helpful in this regard.

a) Review of risk categorization of customers should be carried out annually for high, three years for medium and as on need basis for low risk customers and,
b) Review of risk categorization of customer should be carried out as per mentioned in chapter 4.
c) Risk profile may be upgraded or downgraded during the review, while reviewing employee must consider formal or informal information of the customer and should be updated in the core Banking system also.
d) Bank must monitor the transactions and purpose of cards issued and electronic devices. During monitoring of such card transactions, if any suspicious activity is found, Bank shall block the card immediately.
e) Bank must update the Information of customer required by FIU. At the time of up-gradation of customer, the Bank must obtain only such information other than documented information.

f) While opening the new account, Branch manager should review and authenticate the completely filled up KYC form independently with trustworthy source and maintain such documents.

g) All branches should update the KYC form (prescribed in this policy) for all the accounts within the time frame given by the Senior Management.

h) Must obtain proper identification documents of the customers/originator get filled up CDD form and verify the authenticity every time in following situations.

- Customer request for establishing business relations with the Bank.
- Carrying out series of transactions below the threshold.
- Money transfer through wire /swift / TT.
- There is a suspicion of money laundering or terrorist financing.
- If there is doubt on previously submitted identification document.

i) Suspension of relationship with the Bank

In case of an account already opened where a branch has not been able to apply appropriate CDD measures due to non-furnishing of information and/or non-co-operation by the customer, the branch should consider closing the account or terminating the Banking business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Further, decision in such cases should be taken by the branch head only, after taking into consideration all the relevant facts. Such transactions should be reported to FIU, through AML/CFT Department Head Office, as suspicious transaction. Concerned Officer should regularly obtain and monitor the list of Terrorist person or group of person or entity from the website of Home Ministry.

Chapter 6:

Monitoring of Transactions

Ongoing monitoring of transactions done by the customer or real owner/beneficiary from the point view of their legacy/genuineness is an essential element of effective RBCDD procedures.

a) Cash Deposits of Rs 10 lacks and more from a single customer
   - Branch should ensure that KYC form is properly updated
   - Obtain self-declaration of source of income from the customers
   - Customer's declaration mentioning that the money is not received from terrorism, drug and weapons smuggling, human trafficking, and such organized crime is also acceptable.

b) Branches should pay special attention to
   - All complex, unusually large transactions and
   - All unusual patterns, which have no apparent economic or visible lawful purpose.
   - Transaction done by Individuals, Institutions of the country not fully or partially following the international standards of Anti Money laundering and financing in terrorist activities.
   - The background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch should be properly recorded.
   - These records are required to be preserved for five years as is required under Asset (Money) Laundering Prevention Act, 2008. Such records and related documents should be made available to help auditors in their work relating to scrutiny of transactions and also to NRB/other relevant authorities.

c) Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the Branch. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being washed through the account. Branches should report transaction as suspicious when there are reasonable and sufficient grounds for creating suspicion irrespective of the transaction threshold (1 million) to AML/CFT Department.

d) Such transactions being of suspicious nature should be reported to the FIU immediately through AML/CFT Department.

Chapter 7:

Wire Transfer

Wire transfer is a quick method for transferring funds between Banks. Wire transactions may be within the national boundaries of a country or cross border. The Bank may act as either beneficiary financial institution or ordering financial institution. As wire transfers do not involve actual movement of currency, they are considered as a rapid and secure method for transferring high value amount from one location to another. It has been the most preferred route for transfer of funds across the globe. Following procedures should be observed while executing a wire transfer transaction. In case the wire transfer requesting customer (originator of transaction) could not provide the said details, such transactions should be considered as suspicious transactions and reported to FIU accordingly.

a) In case of any inward/outward remittance, must obtain and verify genuineness of information about the originator:
   - Name of originator,
   - Account number of originator (if not, then any unique reference number),
   - Originator identification number and address. (if not, date of birth, date of place or Citizenship number)
   - Name and Account Number of the beneficiary or if not Account Number, Unique Reference Number.
   - Name and Account Number of Ultimate Beneficial Owner (If account number is not available; any unique transaction reference number which can be used for identifying the transaction).
   - For any wire transfer; must obtain and verify the information as per Point b) above. However, for wire transfer of NPR 75,000 or below, if details of Ultimate beneficial owner is not available; that detail can be omitted.

b) In case of domestic wire transfer, any of following document should be obtained.
   - Information accompanying all domestic wire transfers must include complete originator information or payment instruction, or

- Account number of originator (if not, then any unique reference number) or payment instruction. In case of requirement from Head office or FIU, branch should be able to provide detail of such wire transfer immediately.
- Include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering financial institution should be required to make the information available within 3 business days or as per request either from the beneficiary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

c) In case of cross-border wire transfer,
   - Transaction must be accompanied by accurate and meaningful originator information.
   - Where several individual transfers from a single originator are processed the batch file should contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country, provided they include the originator's account number or unique reference number.
   - Verification of the information pertaining to its customer where there is a suspicion of ML/TF.
   - Details of transaction provided by originator if found to be associated with local wire transfer, details of originator must be documented and if such transaction are received frequently from same originator and does not match with KYC documents shall be reported to FIU as Suspicious transaction.

d) Continuous monitoring of compliance/non-compliance of AML/CFT provisions by Remittance Agents shall be done and Detail of remittance agencies of the Bank shall be updated in the Bank's website regularly.

e) While issuing card or acquiring off-US card, and while transferring fund through cards, the detail of card holder should be maintained.

f) Inward remittance without complete detail of sender/originator shall not be paid to the beneficiary. Bank should inquire for complete details and/or Exemption of Details from the originating Bank. If the originating Bank does not provide complete details of sender, such transactions must be rejected or suspended and shall also be reported to FIU as suspicious.

g) Required to keep a record, for at least five years, of all the information received related to originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer.

h) Bank (if Bank is the beneficiary institution) should take reasonable measures to identify cross border wire transfer that lack required ordering or beneficiary information. Such measures may include post event monitoring or real time monitoring where feasible. If full details of ordering and beneficiary customer is not available in wire transfer transactions, such wire transfer transactions should be considered as a risk for money laundering and terrorist financing. In such cases, Bank should avail the omitted details from ordering institution. If omitted information is not received and full details of ordering customer is lacking; Bank should consider such transactions or related transactions as suspicious and should report to FIU. Additionally, Bank can reject such transactions. In above cases, Bank can prohibit to conduct transactions with such ordering institutions that do not comply with this direction.

Chapter 8:
Correspondent Banking

Correspondent Banking is the provision of Banking services by one Bank (the "correspondent Bank") to another Bank (the "respondent Bank"). Used by Banks throughout the world, correspondent accounts enable Banks to conduct business and provide services that the Banks do not offer directly. Correspondent accounts that merit particular care involve the provision of services in jurisdictions where the respondent Banks have no physical presence. However, if Banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to the range of risks i.e may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

Bank should gather sufficient information about the respondent Banks to understand fully the nature of the respondent's business. Factors to consider include:

a) Information about the respondent Bank's management, nature of business, major business activities, where they are located and its money-laundering prevention and detection efforts;
b) The purpose of the account; the identity of any third party entities that will use the correspondent Banking services; and the condition of Bank regulation and supervision in the respondent's country.
c) Banks should only establish correspondent relationships with foreign Banks that are effectively supervised by the relevant authorities. For their part, respondent Banks should have effective customer acceptance and KYC policies.
d) In this regard, Bank shall pay special attention at the time of establishing the correspondent relationships such as Registration documents, Operating License, Completed AML questionnaire, Wolfsberg questionnaire, List of Board of Directors & Management Profile, Ownership Structure, AML Policy & Procedure, US Patriot Act Certification etc.
e) In particular, Banks should refuse to enter into or continue a correspondent Banking relationship with a Bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell Banks).
f) Bank shall pay particular attention when continuing relationships with respondent Banks located in jurisdictions that have poor KYC standards or have been identified as being "non-

cooperative" in the fight against anti-money laundering and if found to be non-compliance of AML-CFT measures, then the relationship must be terminated.

g) Bank shall establish that their respondent Banks have due diligence standards as set out in this paper, and employ enhanced due diligence procedures with respect to transactions carried out through the correspondent accounts.

h) Bank shall be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf (e.g. payable-through accounts). Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated accordingly. The payable-through accounts are prohibited by this policy.

i) Approval must be taken with Chief Executive Officer before establishing correspondence Banking relations.

1 Resubmission Policy

Once a transaction is rejected by Bank due to sanctions / money laundering / terrorist financing concerns, concerned department / branch shall maintain the record of such rejected transactions and shall not accept the same resubmitted after stripping off information. Stripping off is the deliberate act of changing or removing material information from payments or instructions, making it difficult to identify payments or to connect them to sanctioned parties, individuals or countries. Bank monitors such transactions though are very rare and less in number. Moreover, the branch shall maintain record of the transactions rejected by correspondent Bank and report to AML/CFT Department. The branch needs to recheck the said transaction before resubmitting such transactions.

2 Nested or Downstream Correspondent Banking

Nested or Downstream Correspondent Banking accounts involve a Bank obtaining access to a financial system by anonymously channeling funds through the correspondent Bank of another foreign institution, rather than having its own accounts. The Bank does not provide downstream (or nested) correspondent Banking account service to the customers.

Chapter 9:
Record Keeping

Records of all transactions with customers and beneficial owners, STR and TTR should be retained for at least five years from the date of transaction unless any longer period recommended by regulatory authority. The necessary records on transactions, both domestic and international, for at least five years following completion of the transaction. The records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction. The CDD information and transaction records are available swiftly to domestic competent authorities upon appropriate authority. This provision applies whether the account has been closed. Retention may be in the form of original documents, discs, tape or microfilm.

In situations where the records relate to ongoing investigations or transactions that have been the subject of disclosure, they should be retained till conclusion of the investigation subject to minimum retention period of five years.

Detail of all transactions should be retained in such a way that these could be evidence in case of court case. Transaction records should contain at least following: -

a) Customer Name (including beneficiaries) and address
b) Transaction's nature and date
c) Transaction currency and denomination.
d) Account number involved and its type.
e) Record of identification e.g. Copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence.

The information collected from the customer should be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Staffs should, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the NRB guidelines issued in this regard. If any information to be provided to court as evidence, approval from Chief Executive Officer should be obtained.

Chapter 10:

Threshold Transaction Reporting

A Threshold Transaction Report (TTR) is a report of deposits, withdrawals, exchange of currency, or other payment by, though, or to the Bank which involves a transaction more than Rs. 1 million in a day. The threshold amount may be reached by a single transaction or by a series of transactions in cash into a single account or by a single customer over a period of one working day. It is an aggregate transaction in cash exceeding the prescribed threshold.

Explanation: Indications of when a series of smaller amounts combine to form a "composite" transaction that exceed the prescribed threshold are the following:

- The period within which such a series of smaller transactions take place
- The fact that the series of transactions consists of a repetition of the same type of transaction e.g. cash payments or cash deposits;
- The smaller amount transactions involve the same person or account holder, or relates to the same account.

Cash does not include negotiable instrument, nor does it include a transfer of funds by means of cheques, Bank draft, electronic funds transfer, wire transfer or other written order that does not involve the physical transfer of cash. These methods of transferring funds do not fall within threshold reporting obligation.

1 Following transactions are considered as Threshold Transactions

a) Deposit or withdrawal of Rs 1 million or more into or out of the same account under single cash transaction or in a series of cash transactions per day.

b) Inward or outward cross border transaction of Rs 1 million or more into or out of the same account in one transaction or in a series of transactions in one day or inward or outward remittance Rs 1 million or more by a customer (in case of non-account-holder customer) in one transaction or in a series of transactions in one day.

c) Exchange of foreign currency Rs 500,000 or more by a customer in single transaction or in a series of cash transactions per day.

2 In case of TTR following Guidelines has to be followed

a) AML/CFT Department should file threshold transaction reports to FIU within 15 days from the date of transaction.
b) AML/CFT Department should enter threshold transaction report in the go-AML.
c) Branches should make its customer declare the source of funds in case the transaction exceeds the prescribed threshold.
d) Branches should justify the nature of transactions and the source of fund of transactions in case transaction exceeds the prescribed threshold.
e) Branches should obtain and verify the supporting documents related to TTR only when it is necessary to justify the transaction and retain these supporting documents along with the CDD.

3 Exemption for TTR

Following transactions need not be reported to FIU. However, such exemption is not applicable for any transaction suspicious for financing of AML/Terrorist activities.

a) Transactions done by Government and Government Offices.
b) Transactions done by any entity established under any special act*.
c) Transactions done by Banks, FIs and any public limited companies.
d) Transaction done by insurance companies for re-insurance.
e) Amount transfer through cheque (clearing) from one Bank to another Bank (within Nepal)
f) Transactions done by Offices of United Nations and international organizations.
g) Credit facility provided to customer by Bank and financial institutions.
h) Facility provided to staffs by Bank and financial institutions.
i) The transaction related to Letter of Credit or related payment.

Special Act is implemented by the government to establish any entity like Employee Provident Fund, Citizen Investment Trust, Beema Sansthan, Management Association Nepal etc.

Chapter 11:

Suspicious Transaction Report

This section is intended to highlight situations that may suggest that money laundering is taking place. The customer shall clarify the economic background and purpose of any transaction of which the form or amount appear unusual.

Suspicious Transaction arises from the suspicion created by a specific transaction, which creates the knowledge or belief that the transaction may relate to the legitimization of proceeds from ML/FT activities. Suspicious Activity arises from suspicion relating to general behavior of the customer in question which creates the knowledge or belief that they may be involved in ML/FT activities out of which revenue might be generated.

The goal of STRs filings is to help the Financial Information Unit (FIU) identify individual groups and organizations involved in fraud, terrorist financing, money laundering, and other crimes. FIU requires an STR to be filed by a financial Institution when the financial institution suspects insider abuse by an employee, violations of law or more that involve potential money laundering or violation of existing AML/CFT law, or when a financial institution knows that a customer is operating as an unlicensed money services business.

It is important to note that not all suspicious transactions suggest that a money laundering activity is taking place. However, a combination of such situations may be indicative that money laundering activity is taking place. It is employees' responsibility to ensure that all transactions are handled with due diligence. If it is believed or have a 'gut-feeling' that a money laundering activity is taking place, without confronting the customer, matter should be immediately reported to the Operation in Charge / Branch Manager further reporting to AML/CFT Department at Head Office by submitting the "Suspicious Action / Transaction Report".

Branches should report any suspicious activities/transactions to the AML/CFT Department Head Office. While reporting, the branches should clearly mention the account name, account number of the customer, amount of the suspicious transaction, nature of transaction (Deposit or Withdrawal) and the reasonable grounds regarding why the transactions are considered suspicious. According to Assets (Money) Laundering Act 2064, clause 37, No disciplinary or

administrative action shall be taken against any staff who in good faith submit suspicious transaction report and Bank should protect such staffs from any negative consequences that may arise in process of such reporting.

AML/CFT Department should communicate the issue to the related branches where the customer account has been maintained. Branches are responsible for carrying out the Due Diligence Work on the Customer account:

- Verify the KYC Documents and Beneficial Owner
- Review and verify the nature and amount of the transaction (if TTR threshold is crossed, branches should also follow the TTR Procedures outlined in this Policy) and determine if there are any inconsistencies in the account activities. Also verify the sources of fund.
- The Branch Manager will investigate and determine whether there is a real suspicion, if necessary the Branch Manager may take necessary feedbacks regarding the suspicious activities and then report the same to the AML/CFT Department Head Office.
- AML/CFT Department Head Office should report such suspicious activities to FIU *within 3 days*, as required by Section 7 ”dha” of Assets (Money) Laundering Prevention Act 2013.
- If determined dirty or illegal money, AML/CFT Department will inform the concerned Government Authorities and also can freeze the suspicious amount. The AML/CFT Compliance Officer of the bank should be informed about the suspicious transactions and the actions that have been taken before reporting to concerned Government Authority.

While reporting suspicious transaction to Financial Information Unit, following should be consider the following provisions:

- Specified by Assets (Money) Laundering and Prevention Act 2008 and / or as per this act published in gazette by the government as earning from criminal or related to criminal activity.
- Specified by Assets (Money) Laundering and Prevention Act 2008 as terrorist, terrorism, or related to terrorism.
- Suspicious transaction as specified by FIU directives and illustrated in this policy.
- All suspicious transactions including attempted transactions regardless of the amount of transaction.

Chapter 12:

Terrorist and Proliferation Financing

Terrorism, is a criminal act intended to upset a state of terror in the general public or group of persons for political, philosophical, ideological, racial, ethnic or religious purposes in any unjustifiable circumstance. **Terrorist financing** provides funds for terrorist activity.

Proliferation is the manufacture, control, transport, storing or use of weapon of mass destruction and their related materials (including technologies and dual-used goods used for non-legitimate purposes). Weapon of Mass Destruction is a chemical, biological, radiological, nuclear weapon that can kill and bring significant harm to numerous living beings or cause great damage to artificial structures like buildings, natural structures like mountains or the biosphere

Proliferation Financing is the act of providing funds or financial services which are used in Proliferation. It facilitates the movement and development of proliferation-sensitive items and can contribute to global instability and potentially catastrophic loss of life if weapons of mass destruction are developed and deployed.

Both terrorist and proliferators abuse the informal and formal sectors of the financial system. Terrorists raise fund from legitimate sources such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources such as, drug trafficking, fraud, smuggling of weapons and other goods, kidnapping and extortion. Proliferators operate globally, disguise transactions as legitimate trades, and exploit global markets with weak export controls and free trade zones. Therefore, it is important for financial institutions to develop controls and effective measures to prevent the financing terrorism and proliferation of weapon of mass destruction.

As per ALPA, any individual or institution who is involved in terrorism or proliferation financing; accounts of those customer's should be frozen without any pre notice to customer. While account freezing following should be considered:

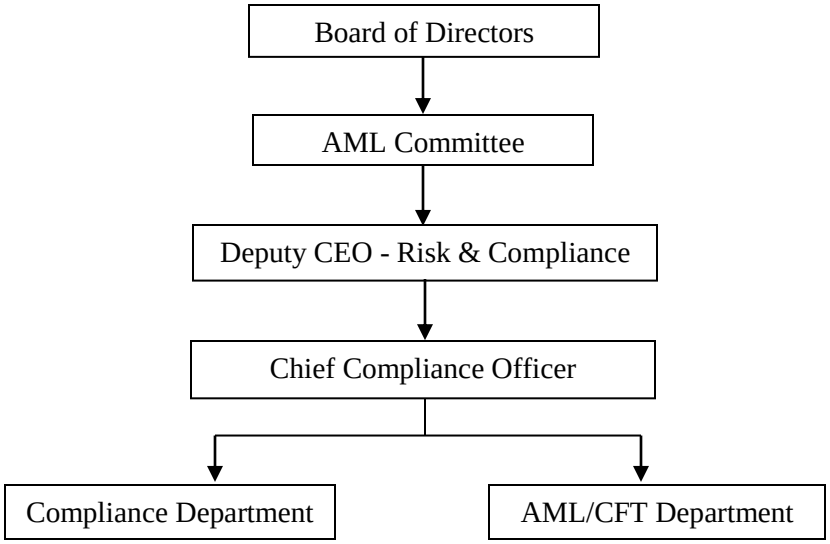
- Screening against sanction list to be conducted.
- The account to total freeze should be directly owned by or being ultimate beneficial owner/ or individual/institution being directly or indirectly involved in terrorism and proliferation.

- The accounts to be total freeze should be owned by individual or institution and act as per instruction of individual or institution who is directly or indirectly involved in terrorism or proliferation.
- During freezing assets; should not be sold, used as collateral or transferred to any individual.
- Bank should report the list of account freeze to regulatory body within 3 days.

Chapter 13:

Internal Controls

In order to perform effective management of AML/FT risks, board level AML Committee of the Bank shall provide governance and oversight of the adequacy and effectiveness of management of ML/FT risks. They will also ensure that AML/CFT programs are aligned with relevant legal and regulatory requirement and AML/CFT strategy is optimally aligned with international best practices. The AML/CFT management of the Bank shall be carried out on the structure as depicted in following Organogram.



1 AML/CFT Compliance Officer

AML/CFT Compliance Officer (of managerial level) is appointed for implementation of this policy in the Bank. Name, Designation, Address, Qualification, contact number, email address of AML/CFT Compliance Officer shall be informed to FIU for correspondence. The AML/CFT Compliance Officer will also be responsible to ensure proper reporting to FIU.

2 AML/CFT Department

The Bank has created AML/CFT Department under AML/CFT Compliance Officer with necessary staffs as per requirement. The AML/CFT Department will look after the overall compliance of AML/CFT policies and procedures, with direct reporting to DCEO - Risk & Compliance and AML Committee. Following tasks should be performed by AML/CFT Department.

a) The AML/CFT Department shall prepare quarterly report on the compliance of AML/CFT Act/Rules/directives issued by Nepal Rastra Bank and report to AML Committee. Such report shall be submitted to NRB on yearly basis.
b) The AML/CFT Department will prepare Offsite Data Collection Form issued by NRB and report to Bank Supervision Department of NRB on half yearly basis within Magh End and Shrawan End respectively.
c) The AML/CFT Department will prepare Bank Self-Assessment Questionnaire form issued by NRB and reports to Bank Supervision department of NRB on yearly basis within Shrawan end.
d) AML/CFT Department shall submit the Risk Assessment Evaluation Report to Financial Information Unit (FIU), NRB within 15 days of each quarter ending in the prescribed in NRB directive no 19 annexures 19.2
e) AML/CFT Department shall submit STR and TTR to FIU as per prescribed in Chapter 10 and Chapter 11.
f) Prepare report on status of implementation of ALPA, AML rules, NRB directives in Bank and submit to AML Committee on quarterly basis.
g) Prepare report on AML/CFT risk management, status on AML/CFT monitoring system, CDD/ECDD status and submit to AML Committee.
h) Any other reporting to FIU should be responded by AML/CFT Department as soon as possible.
i) Risk Assessment shall be evaluated considering influencing factors such as geographical, customer type, product or service type and delivery channel, etc. Such Risk Assessment Report should be reported to NRB on yearly basis.
j) Implementation of group-wide programs against ML/TF, which should be applicable to all branches and majority-owned subsidiaries, this includes
   - Policies and Procedures for sharing information required for the purposes of CDD and ML/TF risk management;
   - Group-level compliance and AML/CFT functions of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes.
   - Adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

3 Branch

In case of Branches, the Operation in-Charge is designated as “Branch AML Officer” who will be focal point for AML/CFT compliance of this policy and reporting to AML/CFT Compliance Officer. Branches should report any suspicious activity observed from any customer to AML/CFT Department immediately.

4 Human Resource Department

Human resource department should conduct proper screening to ensure high standards when hiring employees. The department should coordinate overall AML/CFT related training to all staffs.

5 Internal Audit Department

Internal audit department should conduct independent audit function to test the effectiveness of AML/CFT program (including subsidaries).

6 Business Units \ Departments

The business units \ departments should identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Each respective business units \ departments should be required to:

a) undertake the money laundering and financing terrorism risk assessments prior to the launch or use of such products, services and technologies.

b) take appropriate measures to manage and mitigate the money laundering and financing terrorism risks.

7 Subsidiaries and Foreign Branches

The foreign branches and majority-owned subsidiaries should apply AML/CFT measures consistent with the home country requirements, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements the foreign branches should require to apply appropriate additional measures to manage the ML/TF risks, and inform their home supervisors.

Chapter 14:

Roles and Responsibilities

1 Roles and Responsibilities of Board

The Board of Directors shall be responsible for approving the policies ensuring the appropriateness, sufficiency and effectiveness of the policies adopted by the Bank based on the overall risk level of the Bank on prevention of money laundering and financing of terrorism

2 Roles and Responsibilities of AML Committee

The Committee will be responsible for ensuring effective operation of AML functions. The responsibilities of the Committee with respect to these risks include the following:

a) To present the review report of implementation status according to Assets (Money Laundering Prevention Act 2064, Assets (Money) Laundering Prevention Rule 2073 and NRB Directive 19 to the Board.

b) To discourse on procedural implication of Assets (Money Laundering Prevention Act, 2064, Assets (Money) Laundering Prevention Rule, 2073, NRB Directive 19 and recommendation of Financial Action Task Force in internal policy and procedure and its implementation.

c) To discourse on proper adequacy on management information system (MIS) on monitoring for prevention in money laundering and financing on terrorism activities and provide necessary suggestions to the Board.

d) To implement the customer identification and customer acceptance policy for proper identification of Political Exposed Persons and Ultimate Beneficial Owner according to risk categorization of customer.

e) To provide report regarding implementation status of Bank's internal policy, Assets (Money Laundering Prevention Act 2064, Assets (Money) Laundering Prevention Rule 2073 and NRB Directive 19 to the Board on a quarterly basis.

f) To obtain report from the management and discourse and recommend to the Board;

- Report on AML/CFT risk management
- Report on the effective use of Management Information System (MIS) regarding KYC update, CDD, ECDD, details of PEPs

- Review on AML/CFT related remarks by Internal Audit Report, External Audit Report and NRB inspection Report and corrective measures to be taken in policy and procedural documents of the Bank.

g) The detail information regarding the analysis of ML/FT risk regarding induction of new services, Procurement of IT system, Wire Transfer, e-Banking and mobile Banking (including QR code), fund transfer from mobile wallet and other transactions through online and its improvement in policy and procedure of Bank.

h) To recommend the Board on risk management on ML/FT on regard the consequence of national and international level AML/CFT news and incidents.

i) To initiate and manage knowledge sharing programs on AML/CFT to Implementing Officer, Shareholder holding 2% or more shares of the Bank, Board of Directors, Management Team and staffs related to AML/CFT.

j) To review and recommend periodic review of AML/CFT policy of the Bank to the board.

k) To ensure the proper functioning of AML/CFT system, risk management of ML/FT risk, suspicious action or transaction monitoring and necessary reporting to regulator and discourse the outcome to the board.

l) To discourse the status on a regular basis on reports submitted to FIU and NRB not contradicting with the provision mentioned in Assets (Money) Laundering Prevention Act, 2064 section 44 Ka.

m) Approve annual AML/CFT Program and Budget on risk based approach for combating money laundering and counter measuring of financing of terrorism.

3 Roles and Responsibilities of Senior Management

a) Ensuring that sufficient resources and required access to information, documents and staffs have been arranged to carry out compliance functions efficiently and effectively.

b) Promote compliance as a culture and consider AML/CFT compliance as a basic ethic of doing business.

c) Other discretionary authorities shall be exercised as delegated in the Policy or by the AML Committee from time to time.

4 Roles and Responsibilities of AML/CFT Compliance Officer

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 FIU through letter or electronic means of communication like fax, email,
d) Provide information about transaction of the branch offices to the FIU in a regular basis.
e) Work as a link, counsel and guide for Bank management and staffs on AML/CFT Department.
f) Create environment and get resources for AML/CFT compliance by proper counseling to the top management.
g) Ensure good coordination between operations and top management.
h) Designate or make such management that all offices/branches work in coordination and comply their responsibilities.
i) Ensure that KYC/CDD properly conducted, risk well managed.
j) Ensure that reporting is properly made.
k) Ensure that staffs are well aware and trained on AML/CFT and most particularly on CDD, Risk management and STR detection.
l) Save institution from any type of regulator and other actions.
m) Contribute to the national AML/CFT compliance and objectives therein.
n) Other functions delivered by the FIU.
o) Reporting of TTR/STR.
p) For implementation of act, regulation and directive regarding to AML/CFT, AML/CFT Compliance Officer can demand any information/documents to concerned departments. In case of denial, AML/CFT Compliance Officer has the right to recommend to the Bank for departmental actions and such report to be presented to FIU.

5 Roles and Responsibilities of AML/CFT Department

a) Implementation and periodic review of the policy. Dealing with any queries on its interpretation.

b) Providing AML/CFT compliance related reports like suspicious transaction reports, threshold transactions reports, self-evaluation questionnaire, Bank related data etc. to regulatory authority on a timely manner

c) Keeping abreast of all technical and regulatory developments on money laundering related matters and advising concerned staffs of any changes required in the policy or SOP.

d) Ensuring that all are aware of their responsibilities and obligations, adequately trained in relevant aspects of anti-money laundering processes.

6 Roles and Responsibilities of Designated Staff at Branch

The Operation in-Charge are designated staff assigned for effective management of Money Laundering and Financing of Terrorism risks in the branch level as Branch AML Officer with reporting to AML/CFT Compliance Officer for AML/CFT related issues.

a) Operation in-Charge shall be responsible for ensuring proper implementation of control, monitoring and reporting procedure across their respective branch to prevent ML/FT as Branch AML Officer.

b) Liaison between AML/CFT Department and the Branch for AML / CFT related task / activities.

c) Responsible for executing the duties as required by SOP framed under this policy from time to time.

d) Other major duties shall be as follow:

- CDD / ECDD related responsibility
- Suspicious Activity Reporting to AML/CFT Department
- KYC compliance related responsibility
- The letters of regulatory authority and enforcement agencies related responsibility
- Trust AML Solution related responsibility
- Other roles and responsibilities covered in their job description.

7 Roles and Responsibilities of Operation Department

a) Provide support to the AML/CFT Department as and when required.

b) Work in close coordination with AML/CFT Department regarding customer due diligence.

8 Roles and Responsibilities of Internal Audit Department

a) Conduct compliance audit of this policy at least annually and submit report to Audit Committee.

9 Roles and Responsibilities of Business / Department / Unit Heads

a) Department/Business/Unit Heads shall be responsible, under the area of their control, for ensuring proper implementation of control, monitoring and reporting activities designed to prevent money laundering and terrorist financing.

b) Responsible to reasonably assure that staffs under their control have required knowledge and are not involved in any money laundering and terrorist financing activities.

10 Roles and Responsibilities of Individual Employees

a) It shall be the responsibility of every individual employee of the Bank to remain vigilant to the possibility of money laundering / terrorist financing risks through use of Bank's products and services.

b) Any staffs who come to know about the involvement of Bank's staff or any of its customers in money laundering or terrorist activities must report to the higher management of the Bank following standard procedure framed under this policy and shall be mandatory role of all staffs of the Bank.

c) All the staffs of the Bank shall adhere code of conduct relating to prevention of money laundering and combating financing terrorism as specified in the clause no 2.4 of this policy.

Chapter 15:

Miscellaneous

1 Compliance Review and Monitoring

Internal Audit Department should conduct compliance audit of this policy at least annually and submit report to Audit Committee.

AML/CFT Department should ensure proper implementation of this policy, review the compliance and submit review report to AML Committee and Chief Executive Officer within first quarter of every fiscal year. Such report shall be discussed in BOD meeting.

2 Review and Amendments

AML/CFT Compliance Officer will review and update this AML/CFT Policy from time to time. The CEO shall recommend for amendment, where deemed necessary, to the Board of Directors for approval.

The provisions, policies and procedures outlined in this AML/CFT Policy, if contradicted with the Directives issued by Nepal Rastra Bank and the Government of Nepal will automatically be amended to the extent of the contradiction and the latter shall prevail.

Bank shall have to analyze and update the risk associated with AML/CFT and shall review/amend the policy and procedure where found necessary within first quarter of each fiscal year and shall update/maintain for record.

3 Repeal & Saving

"AML/CFT Policy" shall repeal earlier AML/CFT Policy, 2022 approved by the board. Any amendment in the laws / rules / regulations / NRB Directives / Circulars or any circulars affecting provisions under these Procedures shall have automatic effect amending such provisions under this Policy.

APPENDIX -1

KYC FORM FOR INDIVIDUAL CUSTOMER

Citizens Bank International Ltd. सिटिजन्स् बैंक इन्टरनेसनल लि.

Screening ID _____ KYC ID _____ Date:

Account Number _____ Client ID _____

Account Holder'sName:			PANNO.
Date of Birth:	Citizenship / Id No.:		IssuingOffice&Date:
Gender:	PassportNo.:		IssuingOffice&Date:
Nationality:			Passport Expiry Date:
Phone No.:	MaritalStatus:	Mobile No.:	Occupation:
Email:			PO Box:

Present Address: Ward No.: Tole: House no.: District: Province No.:	**Permanent Address:** Ward No.: Tole: House no: District: Province No.:
In case of non-residence NRN ID (if applicable): Foreign Address: City/State: Contact No.: Type of visa: Visa expiry date:	**Beneficial Owner** Yes No If Yes, Beneficial Owner Name: Address: Relation: Contact No.

Family Members

SN	Relation	Name&Surname	CitizenshipNo.	IssuingOffice	Date of issue
1	Spouse				
2	Father				
3	Mother				
4	Grandfather				
5	Grandmother				
6	Son 1				
7	Son 2				
8	Daughter 1				
9	Daughter 2				
10	DaughterinLaw (son'swife)				
11	FatherinLaw (ofmarriedwomen)				

Occupation/Business

SN	Name of Firm/Company/Office	Address	Web Site	Post	Expected Annual Income
1					
2					
3					
4					

Are you civil servant /high position /politician /relatives of politician? Yes No

Expected Monthly Turnover: Less than 5 Lakhs Less than 50 Lakhs More than 50 Lakhs

Expected Monthly No. of Transaction: Less than 15 Less than 25 More than 25

Purpose of Account: Remittance Savings Business Others

Source of Fund: Salary Remittance Investment Sale of Asset Rental Income
Business Borrowings Loan Repayment Others (Please Specify) _____

Punished or charged for any criminal activities in the past? □ Yes No

Site map Permanent Address □ Temporary Address

I/ we hereby declare that all the information and documents provided to the bank are true & correct.

Right Left

Thumb Impression

Note: Any document/information if not exists, shall be declared an N/A.

Account Holder's Signature

Bank's Use Only

Supporting Documents (provided by the customer)

Photo of account holder Obtained Not obtained

Photo of beneficial owner Obtained Not obtained

Identification Document: Citizenship Passport Others _____

Address verifying document (Any one): Utility Bill Driving License

(Water/Electricity/Telephone Bill)

Land Ownership Document Rental Agreement Letter from Local Authority Voter ID

Employee ID (Mandatory for Govt. Officials) N/A Yes No

Account Risk Grading:	Information Update in Core Banking System & Accuity Check:
□ High Risk Medium Risk Low Risk	□Yes No
□ HPP PEP	Date Updated on:_____
Name listed in Sanction	Remarks if any:
□Yes No	_____
Remarks information if any:	
Branch Manager	CSD Staff
Date:	Date

While opening deposit account of the client the following information and documents in accordance with the nature of the customer must be obtained which is as per KYC Policy of NRB. However, interview may also be taken, whenever necessary.

APPENDIX -2

KYCFORMFORCORPORATECUSTOMER

Screening ID

KYC ID

Account Number Date:

Client ID

Account Holder'sName:	
Date of Registration:	Registration No.: Registration Office & Date:
	PAN/VAT No. Regd./PAN Expiry Date:
Contact No: Office: Fax: Email: P.O. Box:	Beneficial Owner- Name: Address: Relation: Contact No.:
Registered Address Ward No.: Tole: House No.: District:	**Business Address** Ward No.: Tole: House No.: District:
Business Area:	
Business Objectives:	
Number of Office:Office Location:	
HPP/PEP/NPF:	If yes, remark on affiliation:

Management {BOD Member and Chief Executive)

Supporting Documents (provided by the customer)			**Remarks, If any**
Photo of account operators	Obtained	Not obtained	
Photo of all managerial personnel	Obtained	Not obtained	
Citizenship of all managerial personnel	Obtained	Not obtained	
Registration Document: Registration Certificate MOA/AOA			
Audited Financials of last fiscal year	Yes No Specify theFY.		
Income Tax Clearance of Last Fiscal Year	Yes No Specify theFY.		

S.N	Full Name & Post	Permanent Address	Present Address	Citizenship No./ Issuing Office	Phone/ Mobile No.

Expected Monthly Turnover:	Less than 25 Lakhs	Less than 50 Lakhs	>50 Lakhs
Expected Monthly No. of Transaction:	Less than 25	Less than 50	>50
Purpose of Account:	Business	Others(please specify)	

Corporate Seal

_____

Authorized Signatory

Date:

Location map

I/ we hereby declare that all the information and documents provided to the bank are true & correct.

Company Seal

Bank's Use Only

Account Risk Grading: Information Update in Core Banking System

□ High Risk Medium Risk Low Risk Date Updated on: _____
□ HPP/ PEP

Name listed in OFAC (Name listed in sanction) Remarks if any:
□Yes No
Remarks/ information if any:

_____

Branch Manager CSD Staff
Date: Date:

While opening deposit account of the client the following information and documents in accordance with the nature of the customer must be obtained which is as per KYC Policy of NRB. However, interview may also be taken, whenever necessary.

APPENDIX – 3

Citizens Bank International Ltd.
सिटिजन्स बैंक इन्टरनेसनल लि.
YOUR PARTNER FOR PROGRESS

CUSTOMER DUE DILIGENCE REVIEW

Account Number		Date	
Account Holder's Name:		Account Opened Date:	
Present Address:		Permanent Address:	
Contact No.:	Citizenship Nos.	Issusing Office & Date:	

					Remarks, if any
Address Verifying Supporting documents obtained ?	☐ Yes	☐ No			
Mandate to operate the account given to Third Party?	☐ Yes	☐ No	☐ N/A		
Identification of Third Party Signatory obtained?	☐ Yes	☐ No	☐ N/A		
Residential Address of Third Party Signatory verified?	☐ Yes	☐ No	☐ N/A		
Relationship with the Third Party established?	☐ Yes	☐ No	☐ N/A		
HPP/PEP/NF2F ?	☐ Yes	☐ No	Why?		
Monthly Turnover:	☐ Less Than 5 Lakhs	☐ Less Than 10 Lakhs	☐ Above 10 Lakhs		
Monthly Transaction:	☐ Less Than 15	☐ Less Than 25	☐ Above 25		
Purpose of Account:	☐ Remittance	☐ Savings	☐ Business	☐ Others	
Source of Fund:	☐ Salary	☐ Remittance	☐ Investment	☐ Sale of Assets	
	☐ Donation	☐ Borrowings	☐ Loan Repayment	☐ Others	
Account Turnover In Last Six Months:	Nos. of TXN		Amount Rs.		
Any other remark of accountholder noted?					

As per the points mentioned above,recommended categorization of account: ☐ High Risk ☐ Medium Risk ☐ Low Risk	
Name listed in OFAC (Office of Foreign Assets Control)? ☐ Yes ☐ No	
Reason for Recommendation:	Information Update in Core Bnaking System ☐ Yes ☐ No Date Updated on:_____
_____ Branch Manager Date:	_____ CSD Staff Date:

APPENDIX - 4

MULTIPLE BANKING DECLARATION

Date:- **Fig in '000**

FIs Name and Credit Facilities	Outstanding as on……..	Overdue, if any
1…….Bank		
Working Capital Loan		
Term Loan		
Other Loans		
Non fund based facilities		
2…….Bank		
Working Capital Loan		
Term Loan		
Other Loans		
Non fund based facilities		
2…….Bank		
Working Capital Loan		
Term Loan		
Other Loans		
Non fund based facilities		
TOTAL		

I/We declare that the above furnished information is true and correct. In case of false, we will be liable for any legal action.

Authorised Signatory
Name
Office seal.

APPENDIX -5

Risk Assessment and Analysis related Quarterly Report

Quarter: ….. Year …..

सि.नं	विवरण	संख्या	कैफियत
१	जम्मा ग्राहकको संख्या		
२	पहिचान अद्यावधिक हुन नसकेको ग्राहकको संख्या		
३	पहिचान पुरा नभएका कारण सम्बन्ध अन्त्य गरिएका ग्राहकको संख्या		
४	उच्च जोखिममा परेका ग्राहकको संख्या		
५	मध्यम जोखिममा परेका ग्राहकको संख्या		
६	न्यून जोखिममा परेका ग्राहकको संख्या		
७	बृहत् पहिचान गरिएका ग्राहकको संख्या		
८	उच्च पदस्थ पदाधिकारीको संख्या		
९	वास्तविक धनी पहिचान गरिएका ग्राहकको संख्या		
१०	**goAML Reporting**		
	(क) सिमा कारोबार प्रतिवेदनको संख्या		
	(ख) शंकास्पद कारोबार प्रतिवेदनको संख्या		
११	क्षमता अभिवृद्धि विवरण (क) पदाधिकारी (ख) कर्मचारी		
१२	संचालक समितिमा AML/CFT सम्बन्धी छलफल भएको पटक		
१३	सम्पत्ति शुद्धीकरण निवारण सम्बन्धी समितिको बैठक पटक		

APPENDIX -6

Checklist for Suspicious Action Reporting (SAR)

	Details of Customer
	Name of customer:
	Address:
	Identity card detail & Number:
	Account number (if any):
	Nationality (if applicable):

S.N.	Triggering Indicators	Yes	No
	Cash Transaction		
1	High frequency of cash transactions rounded-off between Rs. 5 Lakhs to Rs. 10 lakhs in a day		
2	Regular customer starts coming in with large amounts of cash (no such previous action)		
3	Does not know or cannot say where the deposit came from		
4	No explanation given for size of transaction or cash volumes		
	Foreign currency exchange		
5	Frequent transaction on behalf of – third party		
6	Frequent transactions in a short period		
	Remittance		
7	Does not know how much the money transferred / Does not want to give an explanation for the money transfer		
8	Receives frequent remittance from unknown/different individuals/organizations		
9	Frequent transactions under Rs. 25,000 to avoid the KYC information		
11	Uses the same address but frequently changes the names involved		
	Electronic Transfers		
12	ATM card previously blocked		
13	Internet / mobile banking related		
	Customer Behavior		
14	For no apparent reason, often comes for transaction at peak hour, after transaction hour or only in crowd		
15	Unreasonable behaviors noticed while opening account and during transaction (nervous, rushed, unconfident etc)		
16	Unwilling or refusing to provide information / documents requested without any clear reasons		
17	Reluctant to meet in person for KYC update		
18	Always requests for transaction to be done too quickly (hurried unnecessarily) requesting to the Operation in Charge and Branch Manager.		
19	Unemployed or has a low paying job but always seems to have a lot of transaction in the account		
20	Tries to maintain close relation unnecessarily especially with the new staff of the bank and also offers tips, gifts.		
21	Shows uncommon curiosity about internal systems, controls and policies.		

Reason for SAR:

Prepared By
Name:

Verified By
Name:

Documents enclosed with SAR

□ Account Opening form□ Cash Deposit / Receipt Voucher
□ KYC form (including linked accounts)□ Foreign Exchange Documents
□ Customer Due Diligence form□ Remittance related Documents
□ Identification Documents□ Others (Please specify) ……

APPENDIX – 7A

Enhanced Customer Due Diligence Form for Retail Customers
Bank Use Only

Date:

Customer Name:	CIF ID:
Account number 1: Account Type: Purpose of Account: □Saving □ Salary □ Business □ Remittance Loan □ Others, specify……..	Account Opened Date:
Account number 2: Account Type: Purpose of Account: □Saving □ Salary □ Business □ Remittance Loan □ Others, specify……..	Account Opened Date:
Occupation:	
Expected Annual Income:	
Anticipated Volume of Transaction:	
Anticipated Number of Transaction:	
Reason for High Risk Categorization:	

Status Verification:

Conducted Screening?: □ Yes □ No

Screening ID:

Screening Result : □ Match ……..…….……. □ No match

Conducted Screening of Mandate, Beneficial owner ? □ Yes □ No

Screening ID:

Screening Result: □ Match …….……..… □ No match

Screening of family details of PEP:

Conducted Screening of Family members?:□ Yes □ No

Screening ID:

Screening Result:□ Match (Please specify)…….……..…. □ No match

Family member Details *(Name of immediate family members)*	Relation	Occupation	Citizenship number	CIF ID

PART A: INFORMATION ON SOURCE OF FUNDS / INCOME

a. Business income:

Name of Institution:_____

□ Trading □ Import/Export □ Manufacturing □ Service related □ Others, specify……

b. Salary

Name of Institution:_____ Designation: _____

□ Government □ Bank □ Insurance □ Pvt. Ltd. □ Others, specify……..

c. Investment earnings:[ ] Trading of shares [ ] Real estate [ ] Others _____

d. Pension: Pension paying office: _____

e. Remittance: [ ] Domestic [ ] International

Received from:

Name: _____ Country: _____

Relation _____

f. Rent:

g. Insurance agent commission: Name of insurance company _____

h. Freelancing: specify …….

i. Agriculture: specify …….

j. Family income:

Name (Person who earns for the family): _____

Relation _____

His/her occupation _____ His/her estimated yearly income NPR _____

k. Others specify……..

PART B: ASSESSMENT

S.No.	Particulars	Status			Remarks
		Yes	No	N/A	
1.	Are following documents collected and verified with KYC information provided in KYC form? i. Identification document : ii. Passport Size Photograph : iii. Identification document of Nominee/Mandate (If applicable) : iv. Photograph of Mandate (If applicable) : In case of joint account, are all the above documents of all the joint holders obtained?				
2.	If any information required in KYC form (Such as house number, telephone number, mobile number, e-mail address, passport, profession/occupation, pan number etc.) are not available, is self-declaration from customer obtained that these information are not available?				
3.	In case of foreigner, a) Is copy of Passport and Visa obtained? Is the expiry date of Passport and VISA Validity marked in Finacle CBS? b) Mention the Passport issuing country and has the screening of the country been done?				
4.	In case of minor, are the following documents collected and verified with KYC formation provided in KYC form? i. Identification document of minor: (Birth Certificate of minor/ Citizenship Certificate if the minor has crossed 16 years of age) ii. Identification document of Guardian:				

	iii. Passport Size Photograph of guardian and minor :				
5.	Is all the information required in AOF and KYC form completely filled and verified (signed by concerned staff)? Please mention the KYC date (YYYY/MM/DD)				
6.	Is all the copy of required documents obtained? If no, what are the pending documents to be obtained?				
7.	Is Photograph ID of account operator recently taken and verified with customer's facial identity and is the signature and thumb impression obtained in the presence of the staff?				
8.	Are position, name and address of customer's occupation/business/employment disclosed clearly?				
9.	Is the customer identified as PEP/PEP Associate? Has the declaration been obtained?				
10.	Has the identification document of all immediate family members been obtained?				
11.	Is location map of the present address adequately drawn to show the present living address?				
12.	Does the customer reside/operate or receive funds from Grey List Country? Specify the Grey List Country……. Mention the Purpose of transaction: □Fee purpose□Travel and tour□living expense □Import/|Export □Gift □Medical □Freelancing □ Others, specify……..				
13.	Is customer introduced by existing account holder /staff in the bank? Staff Name:…….., Employee ID:……..				
14.	Does the customer have Ultimate Beneficial Owner (UBO) who ultimately controls the account? Is the declaration of UBO received from the customer? If yes, has KYC of the UBO been taken and updated in CBS? Mention the name of UBO:……				
15.	Is customer request for opening account in foreign currency? If yes, are ocuments/letter verifying source of foreign currency income obtained?				
16.	Has approval been taken from the competent authority? Mention the approving thority.				
17.	Has details of the accounts been updated in the CBS? All the information such Citizenship number, Employment detail, Salary /Annual turnover, Risk Rating, ould be mandatorily updated as per KYC.				
18.	Is signature of Account Operator(s) scanned and approved?				
19	**Any Relevant Information of the customer:**				

ECDD conducted by:	ECDD verified by:	ECDD approved by:
Staff Name: …… CSD Staff Signature:	Staff Name: …… Operation In-charge Signature:	Staff Name: …… Branch Manager Signature:

Note:

1. **Put a mark Y/N on the status "Yes" or "No"**
2. **Put a tick mark on the status "N/A" if the question doesn't relate to the customer.**
3. **If there is any explanation for the status of the observation, note it down on the Remarks Column.**

APPENDIX – 7B

Enhanced Customer Due Diligence Form for Retail Customers
Bank Use Only
Period: FromYYYY/MM/DDToYYYY/MM/DD

Date:

Customer Name:	CIF ID:
Account number 1: Account Type: Purpose of Account: □Saving □ Salary □ Business □ Remittance □ Loan □ Others, specify……..	Account Opened Date:
Account number 2: Account Type: Purpose of Account: □Saving □ Salary □ Business □ Remittance □ Loan □ Others, specify……..	Account Opened Date:
Occupation:	
Expected Annual Income:	
Anticipated Volume of Transaction:	
Anticipated Number of Transaction:	
Existing Risk Grading:	

Status Verification:

Conducted Re-Screening?: □ Yes □ No
Re-Screening ID:
Re-Screening Result : □ Match ……..…….…… □ No match

Conducted Re-Screening of Mandate, Beneficial owner ? □ Yes □ No
Re-Screening ID:
Re-Screening Result: □ Match …….……. □ No match

Blacklisting Verification:
Blacklisted Date: …….. Reason for blacklist: ……..…… Blacklist removal date: ……..…..

Re-Screening of family details of PEP:

Conducted Re-Screening of Family members?: □ Yes □ No
Re-Screening Result:□ Match (Please specify)…….…….…. □ No match

Family member Details *(Name of immediate family members)*	Relation	Occupation	Citizenship number	CIF ID

PART A: INFORMATION ON SOURCE OF FUNDS /INCOME

a. Business income:

Name of Institution:_____

□ Trading □ Import/Export □ Manufacturing □ Service related □ Others, specify……

b. Salary

Name of Institution:_____ Designation: _____

□ Government □ Bank □ Insurance □ Pvt. Ltd. □ Others, specify……..

c. Investment earnings:[ ] Trading of shares [ ] Real estate [ ] Others _____

d. Pension: Pension paying office: _____

e. Remittance: [ ] Domestic [ ] International

Received from:

Name: _____ Country: _____

Relation _____

f. Rent:

g. Insurance agent commission: Name of insurance company _____

h. Freelancing: specify …….

i. Agriculture: specify …….

j. Family income:

Name (Person who earns for the family): _____

Relation _____

His/her occupation _____ His/her estimated yearly income NPR _____

k. Others specify……..

PART B: Quantitative Analysis

Account Number: …….

S.N	Particular(Quantitative Analysis)	Number	Amount	Remarks
1.	Total Debit Transaction			
2.	Total Credit Transaction			
3.	Total summation of Debit + Credit Transaction			
4.	Average of Debit + Credit Transaction (Annual Turnover)			
5.	Cash deposits greater than or equal to 20 lakhs			
6.	Cash deposits in between the range of NPR 7 lakhs to NPR 9.99 lakhs			
7.	Cash withdrawals in between the range of NPR 7 lakhs to NPR 9.99 lakhs			
8.	Cash withdrawals above 10 lakhs or above			
9.	Account to account transfer (debit) above NPR 50 lakhs			
10.	Fixed Deposit in between the range of NPR 5 lakhs to NPR 49.99 lakhs			
11.	Fixed Deposit greater than NPR 50 lakhs			
12.	Inward Remittance			
13.	Outward Remittance			

Summary of Quantitative Analysis: (analysis such as actual transaction compared with expected transaction volume and number, analysis showing deviation in actual transaction compared with profile of the customer, any kind of unusual transaction observed in the account)

PART C-ASSESSMENT					
S.N.	Particulars	Status			Remarks
		Yes	No	N/A	
1.	Does the customer reside/operate or receive funds from Grey List Country? Specify the Grey List Country……. Mention the Purpose of transaction: □Fee purpose □Travel and tour □living expense □Import/|Export □Gift □Medical □Freelancing □ Others, specify……..				
2.	Is turnover in the account higher than the declaration made by the customer? If yes, is the transaction sufficiently justified? Has the KYC been updated based on the latest justification?				
3.	Does the customer provide necessary evidence for sources of fund upon request? Further, is the evidence of sources of fund disclosed by the customer sufficiently justified to be from the legal source? If not, has the suspicious transaction been reported to the AML/CFT department?				
4.	Does customer intimidate to close account when any information is queried? If yes, has the case been referred to higher authorities as appropriate?				
5.	Has customer submitted a request for account closure, after making additional query about their personal information or transactions? If yes, has the case been referred to the higher authorities at branch or at HO as appropriate? (Kindly describe the matter in remarks column) Has the suspicion in the account been reported to the AML/CFT department?				
6.	Does the customer make large number and/or amount of payments in foreign currency? Are the payments made within the regulatory guidelines and the countries to which the payments are sent are in the list of FATF High Risk Country?				
7.	Does the customer make high number of share transactions?				
8.	Does customer avail any other services apart from Deposit?				
9.	Does the customer use non face to face banking services? If yes, has the bank performed appropriate level of due diligence and monitoring of transaction through non face to face medium?				
10.	Does the customer frequently make high number of transaction just below the threshold of NPR 1 million or in excess of NPR 1 million? Is approval obtained as per operation circular 68 in case of threshold transaction?				
11.	Is thereunusual involvementof unrelated third person in the account? If Yes, name the third party …… If Yes, what is the relation of the customer with the third party? ……				
12.	Does customer make amount transfer from one account to another frequently with the aim of concealing/ layering the transaction?				
13.	Is the nature of transaction conducted in the account different than the purpose disclosed during the account opening?				
14.	Is the account of the customer freeze by the regulatory body? Mention the reason for block status.				
15.	Has any kind of negative information of the customer published in media?				
16.	Does the customer show unusual behavior?				
17.	Is the KYC and UBO detail updated?				

Any Relevant Information of the customer:

SUMMARY
Transaction Pattern: □ Normal □ Unusual Finding: In case of unusual/suspicious transaction, SAR reported to AML/CFT Department? □ Yes □No
Final Risk Grading:□ Low □Medium □High
Reason for final risk grading:

ECDD conducted by:	ECDD verified by:	ECDD approved by:
Staff Name: …….	Staff Name: …….	Staff Name: …….
CSD staff	Operation In-charge	Branch Manager
Signature:	Signature:	Signature:

Note:

1. **Put a mark Y/N on the status "Yes" or "No"**
2. **Put a tick mark on the status "N/A" if the question doesn't relate to the customer.**
3. **If there is any explanation for the status of the observation, note it down on the Remarks Column.**
4. **Kindly conduct ECDD of Operative account only (Saving and Current).**
5. **If the customer has more than 1 account; the analysis for Part B: Quantitative Analysis should be conducted separately for each account and should be attached in the ECDD form.**

APPENDIX – 7C

Enhanced Customer Due Diligence Form for Legal Customers
Bank Use Only
Date:

Customer Name:	CIF ID:
Account number 1: Account Type: Purpose of Account: Business Remittance Loan Others, specify……..	Account Opened Date:
Account number 2: Account Type: Purpose of Account: Business Remittance Loan Others, specify……..	Account Opened Date:
Account number 3: Account Type: Purpose of Account: Business Remittance Loan Others, specify……..	Account Opened Date:
Nature of Business:	
Expected Annual Turnover:	
Anticipated Volume of Transaction:	
Anticipated Number of Transaction:	
Reason for High Risk Categorization:	

Status Verification:

Conducted Screening?: Yes No

Screening ID:

Screening Result : Match ……..…….…. No match

Conducted Screening of Signatories, Directors, Proprietor, POA holder, and Beneficial owner?

 Yes No

Screening ID of related parties: ……..

…….

…….

Screening Result : Match (Please specify)…….…. No match

Screening of family details of related parties if related parties are PEP:

Conducted Screening of Family members?: Yes No

Screening ID of related parties: ……..

…….

…….

Screening Result: Match (Please specify)…….…. No match

Family member Details *(Name of immediate family members)*	Relation	Occupation	Citizenship number	CIF ID

PART A: SOURCE OF FUNDS /INCOME

Please indicate the source of funds (Tick more than one category as appropriate):

a. Business Income:

Nature of business: ……..

b. Business Income:

□ Others specify…….

□ Obtain the annual revenue from the latest tax clearance certificate: NPR…… F/Y……
(*not applicable in case of newly registered organizations*)

PART B: ASSESSMENT

S.N.	Particulars	Status			Remarks
		Yes	No	N/A	
1.	Is all the information required in AOF and KYC form completely filled and verified (signed by concerned staff)? Please mention the KYC date (YYYY/MM/DD)				
2.	AreKYC of all Director/ Proprietor/ CEO/ Chairman/POA Holdertaken? Are following documents collected and verified with KYC information provided in KYC form? v. Identification document: vi. Passport Size Photograph: vii. Identification document of Nominee/POAHolder (If applicable): iii. Photograph of POA Holder (If applicable) :				
3.	Is all the copy of required documents obtained, verified and clear (certificate of Incorporation, Minute, AOA, MOA, PAN, Audit report, Tax clearance certificate etc.)? If no, what are the pending documents to be obtained?				
4.	Does the entity require licenses and permits? If yes, mention i. Type of License taken. ii. Permit / license issuing authority. iii. Permit / license expiry date				
5.	Has BOD authorized to open account and carry out financial transaction and/or internet banking/Debit card transactions to authorized officials of the company?				
6.	Is Photograph ID of account operator/s verified with operator's facial identity and is the signature and thumb impression obtained in the presence of the staff?				
7.	Is location map of the present address of organization adequately drawn to show the present business address and address of account operators, directors and proprietor?				
8.	Does the organization have Ultimate Beneficial Owner (UBO)?				

	If yes, has details of UBO been verified from share lagat (share certificate) including multiple corporate layer and has KYC of the UBO been taken and updated in CBS? Mention the name of UBO below (any other relevant information) (Note: UBO are the individual who controls at least 10% of voting rights with regards to making decisions of the company.)				
9.	Is customer introduced by existing customer/ staff of the bank? Staff Name: Employee ID:				
10.	Is the customer identified as PEP Associate? Has the declaration been obtained?				
11.	Has the identification document of all immediate family members been obtained?				
12.	Does the customer reside/operate or receive funds from Grey List Country? Specify the Grey List Country……. Mention the Purpose of transaction: □Import/|Export □Donation □trade related □Others, specify……...				
13.	Is the customer request for opening account in foreign currency? If yes are documents/letter verifying source of foreign currency income/transaction obtained?				
14.	Has approval been taken from the competent authority? Mention the approving authority.				
15.	Has details of the account been updated in the CBS? All the information such as Registration number, Director/proprietor/account operator/ beneficial owner information, Annual turnover, Risk Rating, KYC review date should be mandatorily updated.				
16.	Is the company stamp and signature of Account Operator(s) scanned and approved ?				

17. **Any Relevant Information of the customer:**

ECDD conducted by:	ECDD verified by:	ECDD approved by:
Staff Name: …… CSD Staff Signature:	Staff Name: …… Operation In-charge Signature:	Staff Name: …… Branch Manager Signature:

Note:

1. **Put a mark Y/N on the status "Yes" or "No"**
2. **Put a tick mark on the status "N/A" if the question doesn't relate to the customer.**
3. **If there is any explanation for the status of the observation, note it down on the Remarks Column.**

APPENDIX – 7D

Enhanced Customer Due Diligence Form of Legal Customers
Bank Use Only
Period: From…….. To ……

Customer Name:	CIF ID:
Account number 1: Account Type: Purpose of Account: Business Remittance Loan Others, specify……..	Account Opened Date:
Account number 2: Account Type: Purpose of Account: Business Remittance Loan Others, specify……..	Account Opened Date:
Account number 3: Account Type: Purpose of Account: Business Remittance Loan Others, specify……..	Account Opened Date:
Account number 4: Account Type: Purpose of Account: Business Remittance Loan Others, specify……..	Account Opened Date:
Nature of Business:	
Expected Annual Turnover:	
Anticipated Volume of Transaction:	
Anticipated Number of Transaction:	
Existing Risk Categorization:	

Status Verification:

Conducted Re-Screening?: Yes No

Re-Screening ID:

Re-Screening Result : □ Match ……..…….…….…. □ No match

Conducted Re-Screening of Signatories, Directors, Proprietor, POA holder, and Beneficial owner?

 Yes No

Re-Screening ID of related parties: ……..

…….

…….

Re-Screening Result : □ Match (Please specify)…….…….…. □ No match

Blacklisting Verification (Firm):

Blacklisted Date: ……. Reason for blacklist: ……..…. Blacklist removal date: ……..

Blacklisting Verification (all related parties**):**

Blacklisted Date: ……. Reason for blacklist: ……..…. Blacklist removal date: ……..

Screening of family details of related parties if related parties are PEP:

Conducted Re-Screening of Family members?: Yes No

Re-Screening ID:

Re-Screening Result: □ Match (Please specify)…….…….…. □ No match

Family member Details *(Name of immediate family members)*	Relation	Occupation	Citizenship number	CIF ID

PART A: SOURCE OF FUNDS /INCOME

Please indicate the source of funds (Tick more than one category as appropriate):

a. Business Income:

Nature of business: ……..

b. Business Income:

□ Others specify…….

□ Obtain the annual revenue from the latest tax clearance certificate: NPR…… F/Y……
(*not applicable in case of newly registered organizations*)

PART B: Quantitative Analysis

Account Number: …….

S.N	Particular(Quantitative Analysis)	Number	Amount	Remarks
1.	Total Debit Transaction			
2.	Total Credit Transaction			
3.	Total summation of Debit + Credit Transaction			
4.	Average of Debit + Credit Transaction (Annual Turnover)			
5.	Total Debit Transaction (Without Standing Instruction-SI)			
6.	Total Credit Transaction (Without SI)			
7.	Total summation of Debit + Credit Transaction (Without SI)			
8.	Average of Debit + Credit Transaction (Annual Turnover) (Without SI)			
9.	Cash deposits greater than or equal to 20 lakhs			
10.	Cash deposits in between the range of NPR 7 lakhs to NPR 9.99 lakhs			
11.	Cash withdrawals in between the range of NPR 7 lakhs to NPR 9.99 lakhs			
12.	Cash withdrawals above 10 lakhs or above			
13.	Account to account transfer (debit) above NPR 50 lakhs			
14.	Fixed Deposit in between the range of NPR 5 lakhs to NPR 49.99 lakhs			
15.	Fixed Deposit greater than NPR 50 lakhs			
16.	Inward Remittance			
17.	Outward Remittance			

Summary of Quantitative Analysis: (analysis such as actual transaction compared with expected transaction volume and number, analysis showing deviation in actual transaction compared with profile of the customer, any kind of unusual transaction observed in the account)

PART C: ASSESSMENT					
S.N.	Particulars	Status			Remarks
		Yes	No	N/A	
1.	Is the customer identified as PEP Associate? Has the declaration been obtained?				
2.	Does the customer reside/operate or receive funds from Grey List Country? Specify the Grey List Country……. Mention the Purpose of transaction: □Import/|Export □Donation □Trade related □Others, specify……...				
3.	Does the customer request for opening account in foreign currency? If yes are documents/letter verifying source of foreign currency income/transaction obtained?				
4.	Are transactions plausible with type of business disclosed by the customer?				
5.	Does the customer provide necessary evidence for sources of fund upon request? Further, is the evidence of sources of fund disclosed by the customer sufficiently justified to be from the legal source? If not, has the suspicious transaction been reported to the AML/CFT department?				
6.	Does customer intimidate to close account when any information is queried? If yes, has the case been referred to higher authorities as appropriate?				
7.	Has customer submitted a request for account closure, after making additional query about their personal information or transactions? If yes, has the case been referred to the higher authorities?(Kindly describe the matter in remarks column) Has the suspicion in the account been reported to the AML/CFT department?				
8.	Does the customer make large number and/or amount of payments in foreign currency? Are the payments made within the regulatory guidelines and the countries to which the payments are sent are in the list of FATF high risk country?				
9.	Does the customer use non face to face banking services? If yes, has the bank performed appropriate level of due diligence and monitoring of transaction through non face to face medium?				
10.	Does the customer frequently make high number of transaction just below the threshold of NPR 1 million or in excess of NPR 1 million? Is approval obtained as per operation circular 68 in case of threshold transaction?				
11.	Is there large volume of cash deposits from a business that is not normally cash-intensive?				
12.	Are there unexplained repeated transactions between personal and business accounts?				
13.	Is there unusual involvement of unrelated third person in the account? If Yes, name the third party …… If Yes, what is the relation of the customer with the third party? ……				
14.	Does customer make amount transfer from one account to another frequently with the aim of concealing/ layering the transaction?				
15.	Has any kind of negative information of the customer published in				

	media?				
16.	Is the account of the company/Director/Proprietor frozen by the regulatory body or any other government institution? If yes, mention the reason and freezing authority.				
17.	Have the customers submitted periodical relevance documents like registration, audited financials, license, etc updated upto this year?				
18.	**Any Relevant Information of the customer:**				

SUMMARY
Transaction Pattern: □ Normal □ Unusual Finding: In case of unusual/suspicious transaction, SAR reported? □ Yes □No
Final Risk Grading:□ Low □Medium □High
Reason for final risk grading:

ECDD conducted by:	ECDD verified by:	ECDD approved by:
Staff Name: …….	Staff Name: …….	Staff Name: …….
CSD Staff	Operation In-charge	Branch Manager
Signature:	Signature:	Signature:

Note:

1. **Put a mark Y/N on the status "Yes" or "No"**
2. **Put a tick mark on the status "N/A" if the question doesn't relate to the customer.**
3. **If there is any explanation for the status of the observation, note it down on the Remarks Column.**
4. **Kindly conduct ECDD of Operative account only (Current).**
5. **If the customer has more than 1 account; the analysis for Part B: Quantitative Analysis should be conducted separately for each account and should be attached in the ECDD form.**