Citizens Bank International Limited

AML/CFT Policy 2021

Table of Contents

Abbreviations

AML:	Anti Money Laundering
CFT:	Combating Financing in Terrorism
APG:	Asia/Pacific Group on Money laundering
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
CIT:	Citizen Investment Trust
DNBPs:	Designated Non-Financial Business and Persons
DCEO:	Deputy Chief Executive Officer
ECDD:	Enhanced Customer Due Diligence
EPF:	Employee Provident Fund
FATF:	Financial Action Task Force
FCY:	Foreign Currency
FIU:	Financial Information Unit
HPPs:	High Positioned Persons
KYC:	Know Your Customer
MAN:	Management Association of Nepal
NF2F:	Non Face to Face Customers
NRB:	Nepal Rastra Bank
OFAC:	Office of foreign assets control
PEPs:	Politically Exposed Persons
RBCDD:	Risk Based Customer Due Diligence
STR:	Suspicious Transactions Report
TT:	Telex Transfer
TTR:	Threshold Transactions Reporting

Chapter 1:
Background on AML/CFT

1 Introduction

This Policy shall be known as the "AML/CFT Policy, 2021" 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 collect 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 also exposed to following risks it fails to prevent the Bank being used for Money Laundering and Financing Terrorism 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. In today's competitive environment, operational excellence is critical for competitive advantage. If AML policy is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, 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 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 AML/CFT, 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 2064 BS (second amendment 2070 BS)
b) Asset (Money) Laundering Prevention Rule 2073 BS
c) Directives on AML/CFT (NRB Directives # 19, amendment Ashad 2077 BS)

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 Chief 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 Chief Compliance Officer and provide the Financial Information Unit with the name, address and contact number of the Chief 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

For the purpose of this guidelines, one shall be deemed to have laundered asset, in case one or any third person acquires, holds, posses, uses, consumes, utilizes or earns or displays or transacts or deals with or causes to do so, in any manner, the asset obtained, held, possessed, directly or indirectly from commission of any or all of the following offence or act or the asset increased from any type of investment of such asset; or converts or disguises or transfers such asset or causes to do so with an intention to conceal, convert or disguise the source, nature, place, ownership, right, disposal of such assets; or obtains, purchases, holds, possesses, uses, consumes or utilizes such asset or causes to do so; or does or causes to do transaction in any form in spite of the knowledge of such asset or with the reasonable ground to believe so; or does or causes to do any kinds of assistance directly or indirectly to transform, change or transfer such asset or causes to do so .

Revenue evasion,

- Organized crime and racketeering(extortion)
- Financing of terrorist activities,
- Offence under existing law on arms and ammunition,
- Offence under existing law on foreign exchange regulation,
- Offence under existing law against homicide, theft, fraud, forging of document, counterfeiting, abduction or hostage taking,
- Offence under existing law on narcotic drug control,
- Offence under existing law on national park and wildlife conservation,
- Offence under existing law against human trafficking and transportation,
- Offence under existing law against child sex abuse and all sex abuse,

- Offence under existing law on cooperative institution,
- Offence under existing law on forest,
- Offence under existing law against corruption,
- Offence under existing law on bank and financial institution,
- Offence under existing law on banking offences and penalty,
- Offence under existing law on ancient monument conservation,
- Offence under existing law of piracy of products (illegal production of duplicates and illegal copyrights),
- Offence under existing law of tax (direct and indirect),
- Offence under existing law of market manipulation and insider trading in stock and commodities market,
- Offence under existing law of election,
- Offence under existing law of telecommunication, advertisements
- Offence under existing law of black marketing, consumer protection,
- Offence under existing law of transportation business, education, health, foreign employment fraud,
- Offence under existing law of sole proprietorship, partnership, company or institutions,
- Offence under existing law of land, housing and assets
- Offence under existing law of citizenship and passport,
- Offence under any other law or treaty which Nepal is a party to, as designated by the Government in Gazette.

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.

- Tokyo Convention on Offences and Certain Other Acts Committed on Board Aircraft, 1963,

- Hague Convention for the Suppression of Unlawful Seizure of Aircraft, 1970,
- Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 1971,
- Convention on the Prevention and Punishment of Crime Against Internationally Protected Persons Including Diplomatic Agents, 1973,
- International convention Against th Taking of Hostages, 1979,
- SAARC Regional Convention on Suppression of Terrorism, 1987,
- International Convention for the Suppression of the financing of Terrorism,1999
- Any Convention against Terrorist Activities which Nepal is a party to.

3.4 Bank and Financial Institutions Act 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.

Additionally, other objectives of this policy are;

a) To set procedures to identify AML/CFT transactions.
b) To make bank's staff aware of the AML/CFT policies and practices.
c) To prevent the opening of anonymous and fictitious accounts.
d) To put a system in place to verify the identity of prospective customers before they are allowed to establish account relationship.

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 asset (Money) laundering or terrorist activities is charged with any one or all of the below mentioned punishment

a) Individuals involved in Asset (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 Asset (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% addition punishment with prevailing all above punishment.
g) Employees not maintaining secrecy 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 asset (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.

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) It shall be the policy of the bank to implement automated AML solutions across its network for effective KYC management, risk assessment, transaction monitoring etc.
d) Refuse / 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 as 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) The Bank will also 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. The line of defense shall act as safeguard of 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 while doing business. Businesses shall own and manage the ML/FT risks arising from the 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 Based Approach

The RBA principals propose identification, assessment, understanding and mitigation of ML/FT risk including explicit consideration to key risk factors such as customers, products/services, transactions, country, geographic areas and coverage of banking activities and delivery channel and with varying degrees of impact and levels of risk. 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 assessment on periodic 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 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. Similarly, 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 and make reporting in given time.
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 staff by law.

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.

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, priorities, 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 Chief 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.

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 AML/CFT 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 his immediate supervisor through Head Operations 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 form 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 sudden transaction as prescribed under clause 7 Ka sub clause (1) Ga of Anti-money laundering Prevention act 2064.

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 Embassy

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 CDD measures where lower risks have been identified, through an adequate analysis of risks by the country. 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, and they reasonably believe that performing the CDD process will tip-off the customer, they should be permitted not to pursue the CDD process, and instead should be required to file an STR.

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.
- Simplified or Enhanced Customer Due Diligence (ECDD) 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 Chief Compliance Officer should be obtained before making a decision.

Chapter 3:
Customer Identification

1 Customer

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.

The bank has established procedures to retain adequate records of identification, account opening and transactions, Identification, 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 fallen on FATF, Asia/Pacific Group on Money laundering (APG), IMF, World Bank, List of terrorist maintained by home ministry and UN 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

(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.

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). 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 his immediate supervisor 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 and 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 SOP 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. 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 and Company Service Providers

7 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 Documentation Guideline

a) Clear record of identity of a person should be maintained while establishing any kind of business relationship with such person or while transacting the amount above the threshold, either in a single transaction or in series of transactions as prescribed by Rastra Bank from time to time by publishing a notice.

b) While identifying the customer as per Sub-Section (1), the person establishing business relationship or having transactions with the bank should submit the following documents. The Documents should be verifiable with originals, clear and understood able.

   (Refer Operation Manual for detail of documents to be received while opening an account)

   - In case of a natural person, his/her name, family surname, copy of citizenship or passport including other necessary documents that substantiate his/her permanent residential address and profession or business.

Nepal Government's permanent employees can operate accounts on submission of Government Identity card.

- In case of the person or firm except those provided in Clause (a), copy of the document certifying incorporation, establishment or registration of the institution, documents that mention name, surname, address, profession, business of board of directors and executive director or proprietor of firm or partners of partnership firm,
- In case of accounts of corporate customers, audited financial report shall be required at the time of account opening and such audited documents shall be demanded upon risk assessment for further update.
- In case of any person/firm/company applying for loan facility from bank, declaration of multiple banking.
- In case of business relation or transactions to be established or made on behalf of someone else, documents relating to principal's identity, address including power of attorney clarifying the business of the principal,
- Name, surname, address of close relative, person or institution benefiting from business transaction,
- In case of transactions made through negotiable instruments, name, surname and address of the issuer and payee of such instrument,
- Other documents as prescribed by the Financial Information Unit from time to time.

(c) A separate record of documents and transactions of each customer, pursuant to Sub-Section (b), including date and nature of transactions, type of account and code number should be maintained.

(d) Use of introducers should carefully assess whether the introducers are “fit and proper” and are exercising the necessary due diligence in accordance with the standards set out in this paper. The ultimate responsibility for knowing customers always lies with the bank. Should use the following criteria to determine whether an introducer can be relied upon:

- it must comply with the minimum customer due diligence practices identified in this policy;
- the customer due diligence procedures of the introducer should be as rigorous as those which the bank would have conducted itself for the customer;
- the bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;

- the bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- All relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the bank, who must carefully review the documentation provided. Such information must be available for review by the supervisor and the financial intelligence unit or equivalent enforcement agency, where appropriate legal authority has been obtained.

9 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:
   - Enhanced Customer Due Diligence (ECDD) - for high risk customers
   - Customer Due Diligence (CDD) - for medium risk customers
   - Simplified Customer Due Diligence (CDD) - for low risk customers
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.

1.1 Enhanced Customer Due Diligence (ECDD) for High 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 & Persons (DNFBPs)
f) Business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the 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) Legal entities transacting on cash only (like Travel Agent, Hotel, Restaurant & Petrol Pump) or transacting through new technology only. For Hotel and Restaurants, the entities should be categorized as High Risk on the basis of transaction volume as per the para 3.5 of chapter 3 of AML Procedure of the Bank.
i) Possible to use corporate vehicle for private property.
j) Complex corporate structure with no clear objective.
k) Company with nominee or bearer shareholders.
l) Massive or unduly intended cash transactions without reasons.
m) 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.)
n) Customers who conducts transaction from electronic medium by systematically important and unusually suspicious.
o) Customers being convicted in any offence or involving moral turpitude from a court.

Branch should conduct ECDD for high risk customers and obtain approval from Chief Operation Officer (COO) or his immediate supervisor for opening such high risk customers. ECDD should

justify of Source of Property as well as Source of Fund and limit of the Transactions. Photocopy of Citizenship of living family members (in Case of minor-identification document) must be obtained of those Customers whose ECDD has to be conducted.

1.2 Simplified Customer Due Diligence for Low Risk Customer

These are the type of customers whose identity and source of income clearly disclosed and the transactions in the accounts by and large 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 Customer Due Diligence for Medium Risk Customers

Those customers not categorized high and low risk are to be classified as Medium Risk Customers.

a) The ultimate responsibility for knowing the customer lies with the Branch, specifically the Branch Manager and the concerned staff handling the customer. All branches shall ensure maintaining and updating of customer risk profile on a continuous basis.
b) List of those customers should be maintained who are not in contact even after regular follow up while preparing CDD.

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 (detail of such countries can be checked in OFAC website).
- 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 Compliance department.

d) Such transactions being of suspicious nature should be reported to the FIU immediately through Compliance 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 from one country to another. The bank may act as either beneficiary financial institution or ordering financial institution or intermediary financial institution as depend upon the case. 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 truthiness 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.

b) For any inward/outward remittance of Rs 75,000/- or above, must obtain and verify information regarding beneficiary: Name of beneficiary, Account number of beneficiary (if not, then any unique reference number which identifies the beneficiary) and keep the record of it.

c) 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.

d) 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 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.

e) 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.

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

g) 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.

h) 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,

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, Wolfsburg 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) Banks should 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) Banks should 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) Banks should 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 Compliance 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 more than Rs 1 million into or out of the same account under single cash transaction or in a series of cash transactions per day.

b) Inward or outward remittance of more than Rs 1 million into or out of the same account in one transaction or in a series of transactions in one day or inward or outward remittance more than Rs 1 million 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 more than Rs 500,000/- 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.

Special Act is implemented by the government to establish any entity like EPF, CIT, BEEMA SANSTHA, MAN, ICAN, 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 block the accounts. The Chief 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.

There are different indicators to detect suspicious transactions. Bank should install or develop and implement the system to detect STR. In order to make the detection and filing of STRs expedient for the purpose of preventing money laundering and controlling terrorist financing, below mentioned guidelines has been made and issued which are as follows;

Detection of Suspicious Transactions using two kinds of information

a) Individual Account's History
    1. Threshold based detection
    2. Situation/activity based detection
b) Transaction information from other accounts in peer group

General Characteristics of Suspicious Financial Transactions

a) Transactions having unclear economical and business target.
b) Transactions conducted in relatively large amount cash and/or conducted repeatedly and unnaturally.
c) Transactions conducted differently from that of usually and normally conducted by the relevant customer.
d) Huge, complex and unusual transaction.

Elements of Suspicious Transactions

a) Transaction deviating from:
    1. the profile;
    2. the characteristics; or
    3. The usual transaction pattern of the relevant customer.
b) Transaction reasonably suspected to have been conducted with the purpose of evading the reporting that must be conducted by the relevant reporting entity.
c) Financial transaction conducted using fund alleged to be attributable to predicate offences.

Indicators of Suspicious Transactions

a) Cash
    1. Cash transactions conducted in an unusual amount from that of usually conducted by the relevant customer.
    2. Transactions conducted in a relatively small amount but with high frequency (structuring).

3. Transactions conducted by using several different individual names for the interest of a particular person (smurfing).
4. The purchase of several insurance products in cash in a short period of time or at the same time with premium payment entirely in a large amount and followed by policy surrender prior to due date.
5. The purchase of securities by cash, transfer, or checks under other person's name.

b) Economically irrational transactions

1. Transactions having no conformity with the initial purpose of account opening.
2. Transactions having no relationship with the business of the relevant customer.
3. Transaction amount and frequency are different from that of normally conducted by the customer

c) Fund transfers

1. Fund transfers to and from high-risk offshore financial centers without any clear business purposes.
2. Receipts of fund transfers in several phases and once accumulated the funds are subsequently transferred entirely to other account.
3. Receipts and transfers of funds at the same or approximately the same amount and conducted in a relatively short period (pass-by).
4. Receipts/payments of funds made by using more than one (1) account, either in the same name or a different one.
5. Fund transfers using the account of reporting entities' employee in an unusual amount.
6. If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.

d) Behaviors of the Customer

1. Unreasonable behaviors of the relevant customer when conducting a transaction (nervous, rushed, unconfident, etc.).
2. Unusual curiosity about internal system, control and reporting.
3. Customer/prospective customer gives false information with respect to his/her identity, sources of income or businesses.
4. Customer/prospective customer uses identification document that is unreliable or alleged as fake such as different signature or photo.

5. Customer/prospective customer is unwilling or refusing to provide information /documents requested by the officials of the relevant reporting entity without any clear reasons.
6. Customer or his/her legal representative tries to persuade the officials of the relevant reporting entity in one way or another not to report his/her transaction as a Suspicious Financial Transaction.
7. Customer opens account for a short period.
8. Customer is unwilling to provide right information or immediately terminating business relationship or closing his/her account at the time the officials of the relevant reporting entity request information with respect to his/her transaction.
9. If anyone, for no apparent reason, often comes for transaction at pick hour or only in crowd.
10. If anyone tries to maintain close relation unnecessarily or unnaturally with the employees.
11. If anyone automatically unnecessarily clarifies or tries to clarify legality of amount or transaction.
12. If customer-conducting transaction looks confused, nervous, hurried, or wants to remain reserved at the time of transaction.

e) Miscellaneous grounds for suspicion

1. If it is evident that any one is earning wealth (including cash) by evading tax, custom duty, land revenue, electricity bill, and water bill, phone bill and any other revenue or government fees.
2. If anyone lives unusual lifestyle compared to his/her economic strength, profession/business.
3. If unreasonable economic growth or economic strength is evident.
4. If no information about the source of income is disclosed or stated or information about the source of income is not satisfactory.
5. If any act or transaction is not found reasonable or is found to have been conducted with irrelevant party or where the transaction has no justifiable purpose.
6. If it is evident that repeated transactions below threshold amount fixed by the FIU for reporting purpose take place.

7. If any transaction is related to any person being investigated against or wanted by Police, CIAA, Tax, Revenue Investigation or any other crime investigating agencies in relation to any crime.
8. If reporting institution suspects any transaction relating to the customer against whom the regulatory authorities including Nepal Rastra Bank, Insurance Board, Securities Board, Stock Exchange, Company Registrar, Registrar of Cooperative, Bar Council, Institute of Chartered Accountant of Nepal, etc., have initiated proceedings.
9. If there is suspicion on the transaction due to the fact that the customer is blacklisted by Credit Information Bureau or the reporting institution itself has placed the concerned customer in a high-risk customer category.
10. The transaction of the customer, where it is known or is evident that any investigation or proceeding has been or is being taken by competent law enforcement or regulatory institution of foreign state.
11. If it is evident that the asset is earned from any offence against or abuse of children, women or destitute or any other individual.
12. If it is evident that the asset is earned from extortion, coercive donation collection or from any forcible means to compel one to pay amount or asset.
13. If it is evident that the asset is earned from offence of smuggling, illegal profession, trade and business, theft, bribery, robbery, piracy, illegal production, misuse or illegal transportation of goods.
14. If it is evident that the asset is earned from the offence relating to arms and ammunition under the prevailing law.
15. If it is evident that the asset is earned from the offences under the prevailing foreign exchange regulation laws.
16. If it is evident that the asset is earned from the offence of murder, theft, fraud, forgery of documents, counterfeiting, trafficking of human beings, abduction and hostage taking under the relevant prevailing laws.
17. If it is evident that the asset is earned from the offences under the prevailing narcotics control laws.
18. If it is evident that the asset is earned from the offences under the prevailing national park and wildlife conservation laws

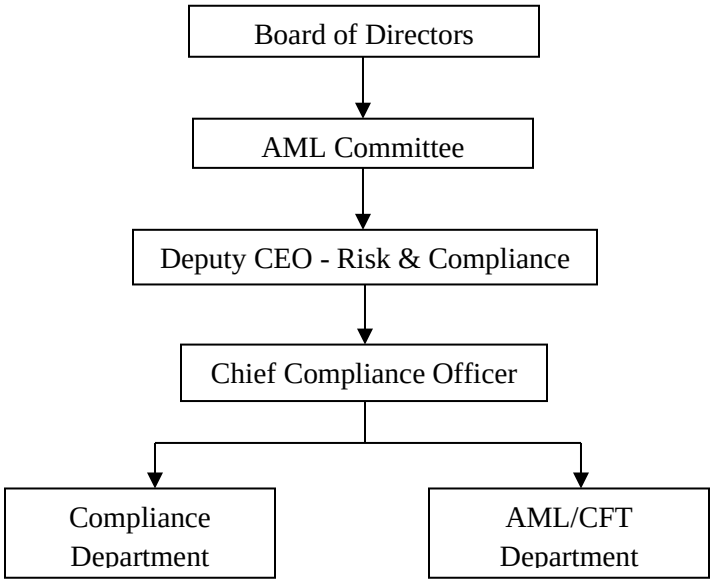
19. If it is evident that the asset is earned from the offences under the prevailing human trafficking and transportation control laws.
20. If it is evident that the asset is earned from the offences under the prevailing cooperatives laws.
21. If it is evident that the asset is earned from the offences under the prevailing forestry laws.
22. If it is evident that the asset is earned from the offences under the prevailing corruption control laws.
23. If it is evident that the asset is earned from the offences under the prevailing bank and financial institution laws.
24. If it is evident that the asset is earned from the offences under the prevailing banking offense and punishment laws.
25. If it is evident that the asset is earned from the offences under the prevailing ancient monuments conservation laws.
26. If it is evident that the asset is earned from the offences under the prevailing consumer protection, black market control and competition laws.
27. If it is evident that the asset is earned from the offences under the prevailing company, commerce, supply, transport business laws.
28. If it is evident that the asset is earned from the offences under the prevailing education, health, drugs, and environment laws.
29. If it is evident that the asset is earned from the offences under the prevailing foreign employment laws.
30. If it is evident that the asset is earned from the offences under the prevailing lottery, gambling and charity laws.
31. If it is evident that the asset is earned from the offences under the prevailing insider trading, fake transaction, securities and insurance laws.
32. If it is evident that the asset is earned from the offences under the prevailing negotiable instrument laws.
33. If it is evident that the asset is earned from the offences under the prevailing election laws.

34. If it is evident that the asset is earned from the offences under the prevailing intellectual and industrial property laws.
35. If it is evident that the asset is earned from the offences under the prevailing communication, transmission, and advertisement laws.
36. If it is evident that the asset is earned from the offences under the prevailing land, house and property laws.
37. If it is found that the asset is earned by the offences under the prevailing immigration, citizenship and passport laws.
38. If it is found that the asset is earned by the offences under the prevailing non-governmental organization laws.
39. Transaction of individual or organization declared to be involved in terrorist or criminal activities by the Government of Nepal or individual or organization listed as terrorist or criminal by United Nation through various resolution or transaction of those directly or indirectly assisting terrorism, terrorist activities, terrorist organization, organized crime, drug offences and any other offences.
40. If transaction seems to be reported based on the news or commentary published in national or international news media about any individual or organization.
41. If it is evident that the transaction is related to any person who is involved in suspicious transaction, likely to promote money laundering, terrorist or any other criminal activities or the transaction that appears to be unnatural or suspicious in any manner.
42. If same address or telephone number/mobile number is provided for different unrelated customers.
43. If such transaction comes under suspicion on the basis of the ground provided by regulator or concerned authority
44. If it is found suspicious on the basis of any other reason or assisting or advising above mentioned activities.
45. If any customer shows unnecessary interest in suspicious transaction or makes unnecessary and unnatural queries about the internal management of such transaction.
46. If there is cross transaction between customers who are not related with each other or any individual transmits or receives amount from unrelated person or business institution's account.

47. If unnaturally huge amount is transferred to the name or account of any foreign citizen, tourist, student, visitor, worker or a person recently migrated to Nepal from the country or region where terrorist organizations operate
48. If there is suspicion that any transaction is aiding criminal activities or receiving amount from such activities.
49. If cash is handled unnatural binding or packaging during transaction.
50. If with no apparent reason there are multiple transactions with the people living in the country where AML/CFT regime is poor.
51. If unrelated third party is unnaturally, unnecessarily involved or is more active in transaction.
52. If anyone tries to complete transaction by paying more without any reason.
53. If person sending money cannot provide even general information about the recipient of money.
54. If there is unnatural inflow or outflow in the name of the firm, company, organization or person involved in such organizations which are not regulated or where no system of economic inspection is developed.
55. If there is repeated transfer of money to and from the name of foreign individual or the individual living outside Nepal.
56. If anyone transfers or receives amount differently from the way of his professional objective or transfers or receives from different place.
57. If there are multiple claims for the amount received from one person.
58. If anyone repeatedly receives multiple amount from different places.
59. If anyone uses different channels to transfer the amount ignoring the usual way.
60. If anyone denies providing identity of the transferor though there are sufficient grounds for him to know such identity.
61. If anyone attempts to transfer or receive amount in a suspicious manner.
62. If a small capital holder tries to transfer or receive unreasonably huge amount.
63. If unable to complete Customer Due Diligence review situation arises
64. Any other transaction the reporting institution finds the grounds for suspicious transaction reporting as per the prevailing law.

Chapter 12:
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 Chief Compliance Officer

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

2 AML/CFT Department

The Bank has created AML/CFT Department under Chief 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 annexure 19.4
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 profile shall be evaluated considering influencing factors such as geographical, occupational, professional, sectoral, customer type, product or service type, nature of transaction, and distribution medium, etc. Risk identified by the government or regulatory shall also be considered. Such Risk Evaluation 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 Chief Compliance Officer. Branches, if observed any suspicious activity from any customer, should report 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 13:
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.

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 Chief 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 to related branches for conducting Enhanced CDD.
p) For implementation of act, regulation and directive regarding to AML/CFT, Chief Compliance Officer can demand any information/documents to concerned departments. In case of denial, Chief Compliance Officer has the right to recommend to the Bank 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 Chief 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 the branch under 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 14:

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

Chief 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 2021" shall repeal earlier AML/CFT Policy, 2020 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.:		Issuing Office & Date:
Gender:	Passport No.:		Issuing Office & Date:
Nationality:			Passport Expiry Date:
Phone No.:	Marital Status:	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	Citizenship No.	Issuing Office	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	Daughter in Law (son's wife)				
11	Father in Law (of married women)				

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

KYC FORM FOR CORPORATE CUSTOMER

Citizens Bank International Ltd. सिटिजन्स बैंक इन्टरनेसनल लि.

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:	

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 the FY.	

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

Income Tax Clearance of Last Fiscal Year Yes No Specify the FY.

HPP/PEP/NF2F:	If yes, remark on affiliation:		
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:	
Address Verifying Supporting documents obtained ?	☐ Yes	☐ No		Remarks, if any
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 नसकेका 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	बृहत पहिचान गरिएका ग्राहकको संख्या		
८	उच्च पदस्थ पदाधिकारीको संख्या		
९	वास्तविक धनी पहिचान गरिएका ग्राहकको संख्या		
१०	सिमा कारोबार प्रतिवेदनको संख्या		
११	शंकास्पद कारोबार प्रतिवेदनको संख्या		
१२	क्षमता अभिबृद्धि विवरण (क) पदाधिकारी (ख) कर्मचारी		
१३	संचालक समितिमा छलफल भएको 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 500K to Rs 1 M 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 100,000 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 pick 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 big tips, gifts.		
21	Shows uncommon curiosity about internal systems, controls and policies.		

Prepared By
Name:

Verified By
Name:

Documents enclosed with SAR

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

APPENDIX – 7

Enhanced Customer Due Diligence

Date:
(DD/MM/YYYY)

Account Name:

Customer ID/Client Code:

Account Number:

Information Checklist
(*Tick in appropriate boxes*)

		Yes	No
1	Does branch conduct ongoing transaction monitoring of customer?	☐	☐
2	Are the transactions normal as per the customer status as presented while opening account?	☐	☐
3	Are KYC documents complete with latest KYC Form and Formalities?	☐	☐
4	Does business nature of customer justify the transactions number and volume?	☐	☐
5	Is branch convenient with client dealing and transactions nature?	☐	☐
6	Are the frequencies of transactions justifiable?	☐	☐
7	Does customer make amount transfer from one account to another frequently with the aim of concealing/ layering the transaction?	☐	☐
8	Is the customer conducted transaction below threshold limit regularly with the aim of escaping from TTR?	☐	☐
9	Have the customers submitted periodical relevance like: registration, audited financials, license etc. are updated up to this year?	☐	☐
10	Is the customer itself the ultimate beneficial owner of the account and its transactions? If No, name the beneficial owner……..	☐	☐
11	Is there third person dealing of accounts regularly other than concerned account holder? If Yes, name the third party……..	☐	☐
12	Is the account duly approved by competent authority while opening? If other than Chief Operating Officer, who has approved it..... Reason for approval……..	☐	☐
13	Is client or its transactions notified or observed as suspicious?	☐	☐
14	Are you comfortable to continue business with the customer in terms of AML/CFT standards?	☐	☐

Mandatory Checklist
(*Tick in appropriate boxes*)

Status Verification : Completed screening check from Trust AML Solutions and attachment of the same *(e.g. Sanction lists / PEP lists / Adverse Media / Hotlist etc.)* Yes □ No □

Name, Date of Birth and Nationality Verification : Customer's Name, Date of Birth and Nationality verified and supported by one of the following accepted documents and a copy held and stamped "Original seen and verified".
□ Citizenship Certificate □ Passport □ Voter's ID
□ Driving License □ Others *(specify)*……...

Address Verification : Customer's Residential Address verified and supported by one of the following accepted documents.
□ Citizenship Certificate □ Passport □ Tenancy Agreement
□ Utility Bill *(specify)*……
□ Physical Verification *(if any, specify)* ……
□ Other *(specify)*……..…...

Additional ID *(for foreign Nationals)* : □ Letter from Embassy □ Voter's ID □ Social Security Card
□ Driving License □ Other *(specify)*……...

Purpose of Account : □ Saving □ Investment □ Remittance
□ Loan Related □ Payroll □ Other *(specify)*……

Source of Funds : □ Salary / Wages □ Income from business □ Income from investments
□ Remittance □ Sale of Assets *(specify)*…… □ Other *(specify)*…….
Obtain the estimated annual remuneration / income or annual sales turnover (*obtain as appropriate*): NPR …….
Comments *(if any)* ……..

Transaction volume : Obtain information on the customer's volume and type of activity to be conducted across the account:

Transaction Types	No of Transaction per Year	Amount per Year	Comment if any
Deposit			
Withdrawals			

Optional Checklist
(*Indicate if customer belongs to any of following categories*)

Special Customer : If the account holder or authorized signatory falls into any of the following categories, tick the appropriate box and specify the required details

- ☐ The customer is Politically Exposed Persons (PEPs) or High Positioned Person (HPP) or closely associated with PEP.
  Please specify details of PEP / HPP position and relationship

  ……

- ☐ A foreign customer residing or operating in grey listed jurisdiction country as per Financial Action Task Force (FATF)
  Please specify country

  ……

- ☐ Customer's source of fund is from grey listed jurisdiction country as per FATF
  Please specify country

  ……

- ☐ Customer's business categorized as high risk like Designated Non-Financial Business Persons, Cash Intensive Business etc.
  Please specify the customer's nature of business / other sources

  ……

- ☐ Account Opened through Non-Face to Face (online) medium.
  Please specify

  ……..

_____	_____	_____
Customer Service Staff	**Branch AML Officer**	**Branch Manager**
Prepared By	**Reviewed by**	**Approved by**

[Note: - Original copy has to be filed in Account Opening File maintained at the Branch and scanned copy of it has to be sent to AML/CFT Department for the record.]

APPENDIX – 8

Simplified Customer Due Diligence Review

Date:

DD/MM/YYYY

Account Number:

Account Holder's Name

Identification Document

ID Type:

ID No:

Issue District:

Issue Date:

Communication

Telephone:

Mobile:

Email:

Source of Fund: ……

Purpose of Account: ……..…

Annual Income: …….……...

Actual Annual Transaction: Dr…….……Cr……...……

Occupation: ……...……

Mandate provided to third party? ……..……

If yes, Verification of ID, address and relationship of third party? …….……..…

Any other remark of accountholder noted? ……..

CSD Staff	Branch AML Officer	Branch Manager