

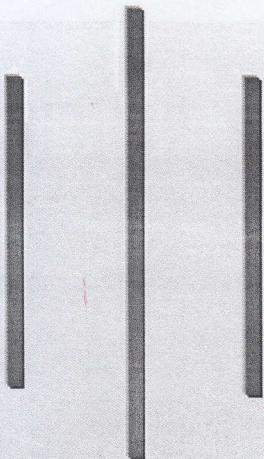


NCC Bank

नेपाल क्रेडिट एंड कमर्च बैंक लि.
Nepal Credit & Commerce Bank Ltd.

Your Business Bank

KYC, AML/CFT Procedural Guidelines- 2018



**Nepal Credit And Commerce Bank Ltd
Bagbazar, Kathmandu**

KYC, AML/CFT Procedural Guidelines-2018

Abbreviations

AML:	Anti Money Laundering
BFIs:	Bank and Financial Institutions
BOD:	Branch Operations Department
BoD:	Board of Directors
CAOU:	Central Account Opening Unit
CAP:	Customer Acceptance Procedures
CBS:	Core Banking System
CD:	Compact Disc
CDD:	Customer Due Diligence
CFT:	Combating Financing in Terrorism
CIP:	Customer Identification Procedures
CSD:	Customer Service Department
ECDD:	Enhanced Customer Due Diligence
FIU:	Financial Information Unit
HRO:	High Ranking Officials
INGO:	International Non Government Organization
IP:	Influential Persons
JV:	Joint Ventures
KYC:	Know Your Customer
NF2F:	Non Face to Face Customers
NGO:	Non Government Organization
NRB:	Nepal Rastra Bank
OIs:	Operation In Charge
PEP:	Politically Exposed Persons
STR:	Suspicious Transactions Report
TTR:	Threshold Transactions Report
UN:	United Nations



KYC, AML/CFT Procedural Guidelines-2018

Approval Sheet

Nepal Rastra Bank (NRB) has amended some of the provision mentioned in NRB Directive No. 19/2074 and some additional provisions are added in existing provision. Subsequent to the amendments of NRB Directive some of the contents/provisions of our internal policy/procedure is auto corrected/superseded and shall be implemented accordingly.

Our existing KYC, AML/CFT Procedural Guidelines has been reviewed as per the regulatory requirement and some changes have been made in existing procedural guideline which are;

- Provision for minor account.
- Provision for NRN account.
- Provision regarding financial report and tax clearance.
- Thumb Impression/Biometric.
- Account of Government Office/Institutions.
- Certifying Documents
- Account of Local Social Committee.
- List of High/Medium/Low Risk Customers.
- Reporting on AML Progress and Risk Assessment.
- Implementation of Go-AML Software.
- Trade Based Money Laundering

As for the
KYC policy 2018,
the revised KYC, AML/CFT
Guideline 2018 is
approved.
Sushil Bhandari

Prepared	Reviewed	Reviewed	Approved
Sushil Bhandari Compliance Unit Date: 10/10/2018	Vinay Pd. Adhikary Head-Compliance Date:	Mukunda Subedi CRO Date:	Ramesh Raj Aryal CEO Date:

KYC, AML/CFT Procedural Guidelines-2018

Table of content:

1. Customers acceptance policy	1
2. Customers identification procedure	3
3. Identification of Walk-In/One-Off customers	9
4. Politically exposed person (PEP's) , High ranking officials (HRO's) and influential person (IP)	9
5. Identification of beneficial owners	10
6. Risk categorization of the customers	12
7. Know your Employee (KYE)	16
8. Customers Due Diligence	17
9. Enhanced Customers Due Diligence	17
10. Correspondent bank and Domestic Bank Relationship	19
11. Threshold Transaction Report (TTR)	19
12. Suspicious Transaction Report (STR) procedure	21
13. Wire Transfer Procedure	23
14. Record Retention in digital form	28
15. Electronic Transaction Monitoring Procedure	29
16. Updating KYC, Conducting CDD, ECDD	30
17. Go-AML Software	31
18. Trade Based money laundering	31
19. Implementation Review and Amendment	36
Annexure-1: Refusal of Account Opening Form	36
Annexure-2: Commitment of Account opening Form	36
Annexure-3: Approval For Personal High Risk Account	37
Annexure-4: Approval For Non-Personal High Risk Account	38
Annexure-5: Customers Due Diligence (CDD) Form	39
Annexure-6: Enhanced Customers Due Diligence (ECDD) Form	40
Annexure-7: Customers Follow Up Form	42
Annexure-8: Suspicious Transaction Reporting Form (For Branches)	42
Annexure-9: KYC/AML/CFT Correspondence Questionnaire	43
Annexure-10: Database Of PEP's Influential Persons and High Ranking Official	50
Annexure-11:Recording Of Correspondence From Various Authority	51
Annexure-12: Details of Board Of Director/Executive Committee	52

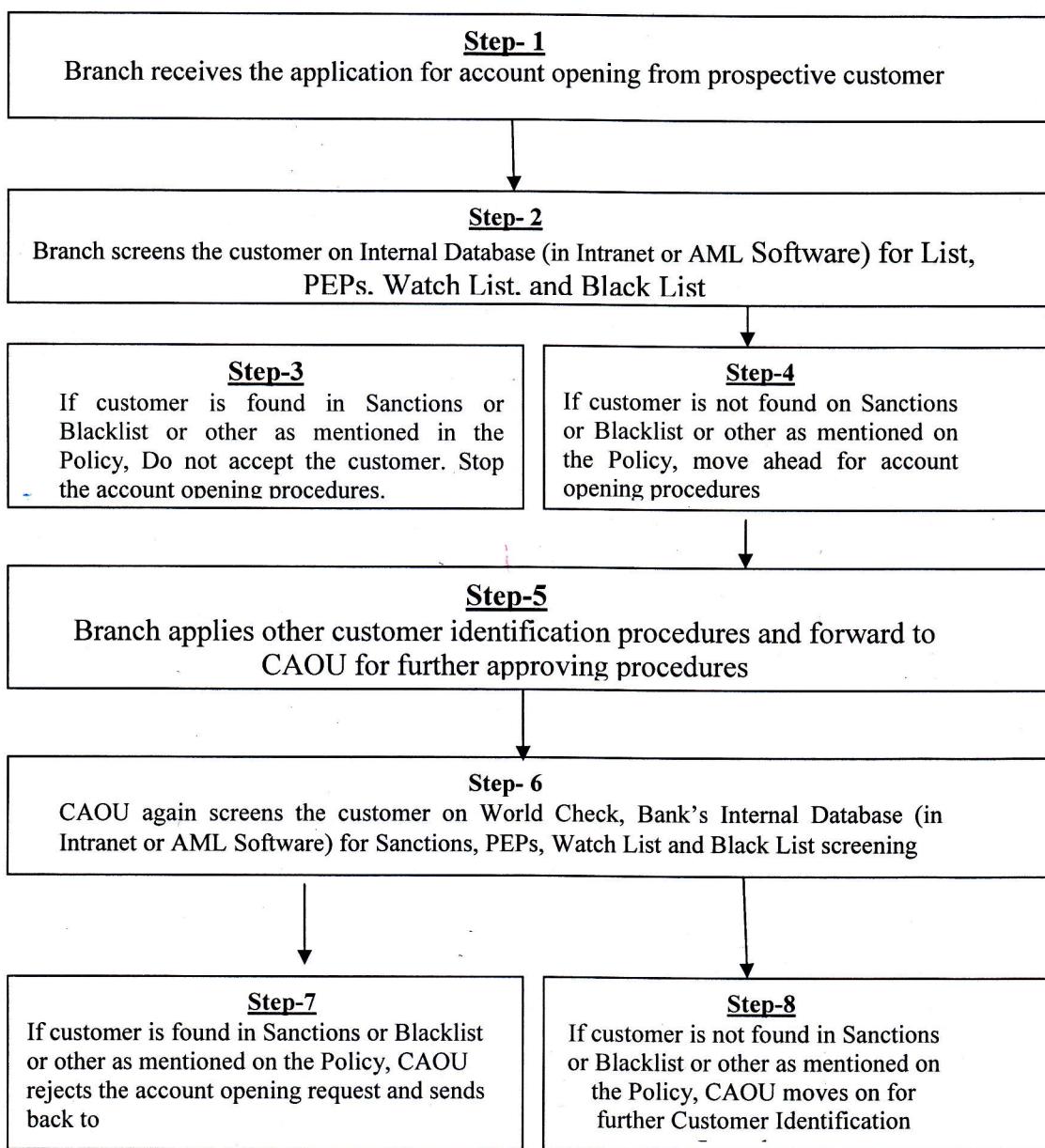
Q/

✓ ✓ ✓

This framework has been formulated for further interpretations and procedural support as required in clause number 22 of KYC, AML/CFT Policy- 2018 (hereafter said as “the Policy”) of the Bank. The framework aims to provide working guidelines for the Internal Control and Regulatory Compliance of KYC, AML and CFT.

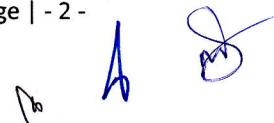
1. Customer Acceptance Procedures (CAP)

In compliance with the clause no 4.2 of the Policy, Bank follows the following procedures on CAP.



KYC, AML/CFT Procedural Guidelines-2018

- A screening facility shall be provided to the branches in Bank's intranet or AML Software for the sanctions, watch list, PEPs, Black List and other types of screening of the prospective customer both on loan and deposits.
- Initially Branch must screen the perspective customer and if found the person with the definition of non acceptable customer, no further process should be done for account opening or other relationship establishment.
- Branch should print the screening sheet and maintain in the account opening file if the account is opened.
- If the customer is not accepted, it has to be informed to the customer with the due reasons and justifications on honest and humble manner as per the **Annexure-1**.
- There should be second tier control at Central Account Opening Unit (CAOU) for the screening and acceptability of the customer. CAOU re-screens the customer as proposed by the branch on World Check, Bank's Internal Database, Watch List, Nepal Government's Sanctions List, Black list.
- If the customer is not found on the list of non acceptability, then CAOU move ahead for other KYC formalities for account opening.
- AML/CFT Unit updates all the sanctions, blacklist and PEPs database and make available to the branches and CAOU daily. Compliance officer always be aware and keep update own self that data are available and updated easily accessible to the branches and CAOU.
- Following type of prospective customer shall **not be accepted** after having detail Customer Identification Procedures (CIP). Such identification procedures shall be conducted both from branch level initially and CAOU further:
 - Who falls under the criteria as given on Clause no 4.2 and other provisions in the Policy of the Bank as restricted to open and operate the account
 - Who does not provide information and documents as needed to identify the customer or does not comply with the general laws of Nepal
 - Whose activity or way of life makes the Bank difficult to know the origin of the money or assets
 - Who does not cooperate the Bank for needful information as needed by KYC, AML/CFT procedures
 - Who is the citizen or resident of sanctions country
- In case of already opened account, customer who does not provide identification documents and other required KYC documents in course of Due Diligence shall not be accepted, and relationship should be suspended or terminated after Customer Due Diligence. Until the account is closed, it must be blocked.





KYC, AML/CFT Procedural Guidelines-2018

- Branch must conduct the Due Diligence on the given frequency as per the Policy. If customer fails to provide the complete set of Customer Identification Documents and information, such relationship should be suspended or terminated on the request of branch, support from Branch Operations Department and approved by CEO.
- If the Suspicious Transaction Reports (STR) or Suspicious Activity Reports (SAR) are reported of any customer three times in a year, relationship with such customer's account may be suspended. The Concerned customer should be informed about the unjustifiable transactions/behavior and cause of the suspension but should not disclose the reporting of STR. CEO's approval should be taken to suspend such relationship.
- The person/entity that is denied as a customer should be recorded in a separate register with the reasons. The record has to be submitted to the Compliance Department on monthly basis. If it is refused from branch level, branch manager has to submit the report. If it is refused from CAOU level, Head/In-Charge CAOU has to report it.

2. Customer Identification Procedures (CIP)

CIP is applied in the following conditions or situations:

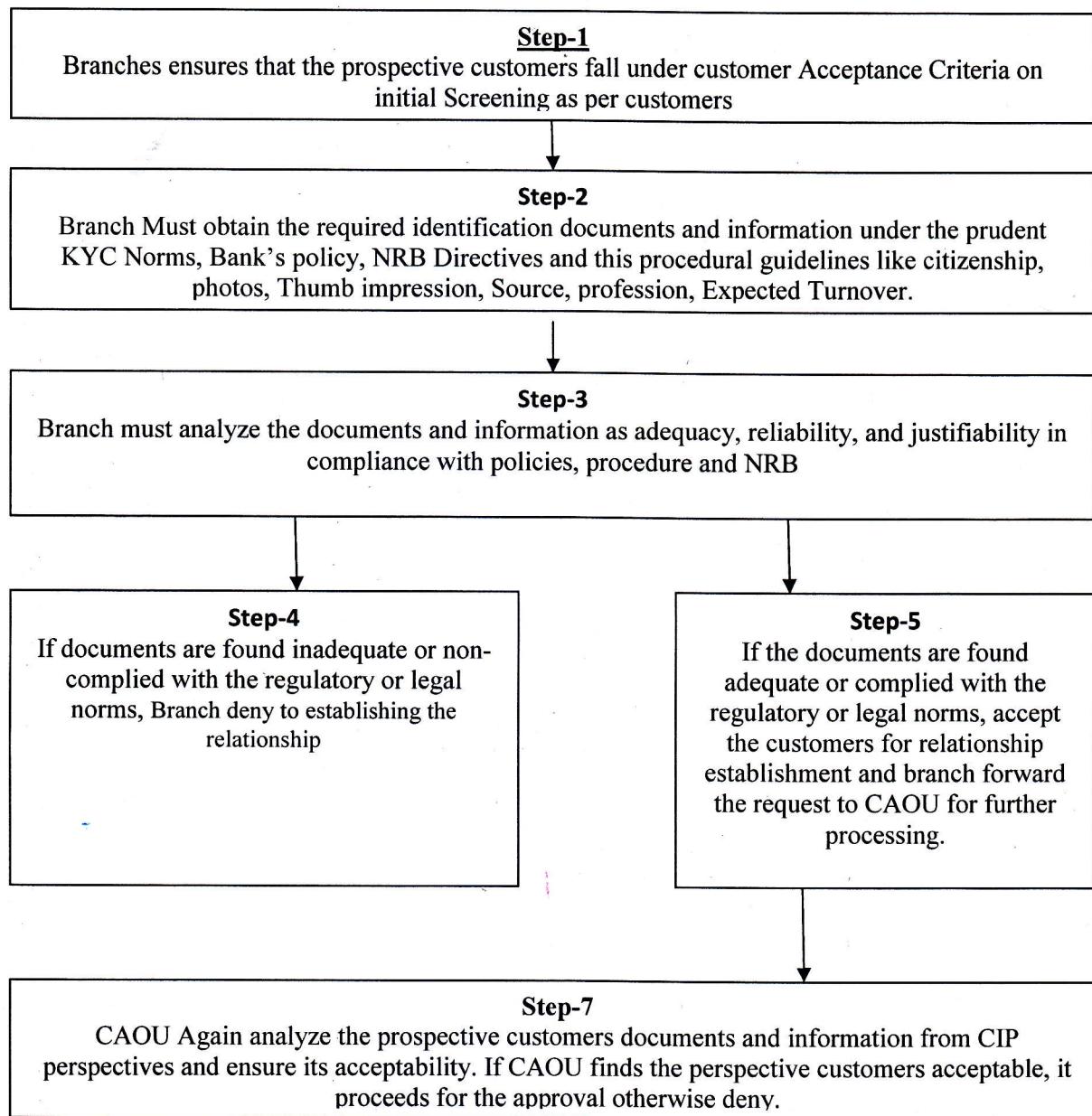
- While establishing banking relationship.
- While carrying out financial transaction with the walk-in or one off customers.
- While need further authenticity or adequacy of the customer existing identification.
- When bank sell third party's products as agents like: Insurance.
- Inward or outward remittances or fund transfer.
- In other conditions where bank feel to take further information/documents.

J

o *A* *S*

KYC, AML/CFT Procedural Guidelines-2018

In compliance with the clause no 4.3 of the Policy, Bank follows the following procedures on CIP.



(Signature)

(Signature)

KYC, AML/CFT Procedural Guidelines-2018

a) Branch conducts the CAP and CIP simultaneously. Branch forwards the request to CAOU if it finds the prospective customer acceptable from both CAP and CIP perspectives with checker and maker modality.

b) Branch ensures that the account opening files are filled up completely and all information as required are updated on Core Banking System i.e. Pumori and Bank's AML Software as well.

c) Branch verifies the information and documents as per the checklist on AML software about the documents adequacy/completeness.

d) **Following details should be obtained from the customer**

1) Full name of the account holder

2) Temporary and the permanent address

3) Date of Birth and Sex

4) Full name of Father mother or father or mother

5) Nationality

6) Occupational details

7) **Expected annual income and expected account turnover.**

8) **Declaration of beneficial owner (if any).**

9) **Thumb Impression or Biometric (Account Operators)**

10) As per the nature of the persons any of the following documents must be obtained:-

- **Nepalese Citizen-** Citizenship Certificate. If citizenship is not submitted then obtain valid passport or Driving License or voter's ID card on temporary basis for maximum 3 months. Citizenship is must ultimately.
- **Minor-** Obtain birth registration certificate, citizenship of the guardian. Citizenship should be obtained when he/she turns out of minor. Fresh photograph, thump impressions and other KYC procedures should be applied when a minor turns into major. **Such account shall be blocked when minor turns into major (i.e 18 years). Similarly, account can be released after the fulfillment of all required documents and handed over the account operating authority in the name of major individual.**
- **Foreign National-** Obtain valid Passport with valid Visa in Nepal
- **Indian Nationals** (not having passport)- Obtain the legal certificate explaining the person as citizenship as per the law of India and must bear certificate number, issuing agency, issued date, place, expiry date and Letter of Indian Embassy/Card issued by Embassy.

- NRN- Obtain Business license or Agreement with employer or appointment letter, Copy of Passport, Valid Visa, NRN ID, Permanent address, Contact address in Nepal.
- Refugees- Obtain the identification document issued by national or international authenticated authority/agencies bearing identity number, issue and expiry date and place of issue.
- If the Customer doesn't have citizenship/legal documents, but promise to submit within a reasonable time period but not more than 3 months and branch seems reasonably justifiable then the account can be opened for Low Risk and Medium Risk customers. Such account shall be closely monitored by maintaining a proper record as per **Annexure 2**. In case the customer is unable to provide the documents later, then such account must be closed. The Dr. Transaction limit shall not exceed NPR 1 million and Cr. transaction limit shall not exceed NPR 10 million for such type of accounts. Above such limit approval of COO must be obtained on exceptional basis. **Further, account under Simplified Due Diligence can be opened against Passport or Voter Card or Driving License without applying transaction limit for not more than next 3 months, valid citizenship copy shall be obtained thereafter. Such account shall be blocked if the customer unable to provide citizenship during the period of 3 months from the date of account opening.**
- If permanent address of the customer deviates from the address mentioned in the citizenship, then obtain the additional supporting documents justifying the permanent address from additional documents like: electricity bill or water bill or telephone bill of NTC or migration (Basai Sarai) certificate, property tax etc. It is not mandatory in case of changes in the address due to reformation of the state level and local level jurisdictions by Nepal Government.

11) As per the nature of the Legal persons following information and documents must be obtained

- Name of the Legal entity
- Full address, Telephone number, email, website and any other contacts of the Business entity
- Nature of the business
- Valid Registration certificate.

KYC, AML/CFT Procedural Guidelines-2018

- Bidhan, MOA, AOA, Chartered, Partnership Deed, Bye-Laws as applicable
- Business license as Applicable
- **Audited Financial Statement as Applicable**
- Tax clearance or Tax submission form
- PAN number or certificate issued for tax purpose by government agency
- *Personal details of the Members of the BoD or Executive Committee or Partners must be obtained along with photo, copy of citizenship and shall undergo Sanction Screening.
- *Personal details of the shareholder holding more than 10% of the shares and shall undergo Sanction Screening.
- Identification documents of signatory of account

*(*Personal details include Name, Designation, Name of wife/husband, Fathers Name, Grand Fathers Name, Permanent Address, Current Address, Telephone Number, Mobile Number, email Address and valid identification document, Please Refer: Annexure-12)*

12) Other than above mentioned for identifying government bodies or organization or international organization, following documents and information must be obtained:

- Decisions to open account or conducting transactions must be obtained,
- Personal details of the account signatory and
- Authority letter for conducting financial transactions must be obtained

*(*As a personal legal identification, Government ID of permanent employee can be obtained from the account operator for the account of Government institution)*

13) Obtain the thumb impression or biometric of the customers while opening of the accounts mandatorily as below:

- **Natural persons:** - Account holder and for mandate too if applicable.
- **Minor accounts:** - Operator of the account
- **Legal persons:** - All the Signatories of the account

e) Certifying Documents:

Where documents are used to verify information, the original must be seen, legible copies taken and certified 'original seen' by the authentic person by

affixing stamp & full signature (NCC Staff includes outsource/contract staff).
The copies must be retained in customer's file.

For Natural persons

- **Nepalese Citizens** - Citizenship or Voters card or Driving license or Passport. For Nepalese citizens not having citizenship recommendation letter from Municipality or Rural Municipality on temporary basis.
- **Minors** - Birth registration certificate or minor identification certificate, citizenship of the guardian
- **Foreign national** - Passport along with valid Visa
- **Indian nationals not having passport:** - legal certificate explaining the entity as citizenship as per the law of India.
- **Refugees:** - Identification document issued by national or international authority.

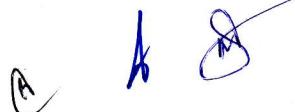
For Legal persons

- Registration certificate and transactions authority letter or renewed certificates
- Business License
- **Latest Audited Financial as applicable**
- PAN Certificate
- Citizenship certificates of account operators,
- The company or entity must submit the citizenship certificates or registration certificates of Board Members or Beneficial owners or other required persons attesting as true copy of original documents. Company secretary or executive chief of the entity should attest the copy.

f) For account mentioned by Nepal Government and its offices, entities established under special act, Institution under ownership of Nepal Government, BFIs licensed by NRB, Insurance company licensed by insurance board and those who have issued shares to general public, UN or offices established under them and foreign Diplomats, Obtain the KYC of the signatory of the account.

g) Requirement to open the account of Local Social Committee;

- Resolutions on the formation of social committee and to open and operate accounts.



- Registration certificate from concerned authority or recommendation from local government.
- Identification documents, contact details and occupational details of all the authorized committee members and KYC documents of account operators must be obtained. For this purpose identification document means copy of citizenship or passport or driving license or voter card.
- Nature of transaction and approximate annual transactions.

3. Identification of Walk-In/One-Off Customer:

Identification of the walk-in/One-off customer, following documents shall be obtained in compliance with the clause no 4.4 of the Policy irrespective of any amount: -

- Copy of Citizenship Certificate. If citizenship can't be obtained then obtain valid Driving License or Voters card or ID card issued by Nepal Government Authorities.
- Contact Number of the Customer.
- Contact Address
- Fathers Name or Mothers Name

For third party depositor, other than account holder, teller shall obtain the Identity Cards (citizenship or driving license or voter's card or Passport or ID card issued by Government Authorities and offices) for amount greater than equals to NPR 1.00 Lac along with the purpose of deposit.

4. Politically Exposed Persons (PEPs) and High Ranking Officials (HRO) and Influential Persons (IP)

In compliance with clause no 4.6 of the Policy, Branches must carry out the following procedures for identification of PEPs, HRO and IP

- Screen the name of the prospective customer in the PEP list of the Bank.
- Compliance Department shall prepare the list of the PEP and update it on continuous basis in Bank's Intranet or AML Software as well.
- Self Declaration can be obtained from the client if s/he is PEPs or not.
- Branch shall send for the checking and verifying if the customers are PEPs, HRO and IP to CAOU. Approval from Head of Compliance on the request of respective business head or Chief Operating Officer (COO) of the Bank is required for establishing the relationship. The Approval must be obtained as per **Annexure-3** for personal Accounts and **Annexure-4** for Non-Personal High Risk Accounts.





***Note: - Undivided Family members and associated persons/entity of PEPs are also considered as PEP. Associated persons/entities are such entities which are directly controlled by PEPs.**

- During updating the KYC, if existing customer is found to be PEP then branches shall obtain the approval and update the information as needed for PEPs.
- Branches must identify the PEPs and their undivided family members
- Branches should maintain the List of the PEPs customers even after s/he is not PEP for the period of five years and must be updated in the CBS. Compliance Department must monitor the status of the PEPs on Quarterly basis. Compliance Department shall Monitor the Transactions of the PEP on regular basis, if found suspicious report STR to FIU.

**National High level Positioned Persons includes President, Vice-President, Ministers, Members of Parliament, Members of Constitutional Bodies, First Class and above officers of Nepal Government, Supreme Court Judge, Top Politicians, Central Members of National level political parties, Top level Management people of Fully or Semi-Government owned institutions*

***International High level Positioned Persons include Presidents of foreign countries, Head of Government of foreign countries, Top politicians of foreign countries, Chief Administrator of foreign countries, Chief judiciary head, Chief Defense head and Top level Management People of Government owned institutions.*

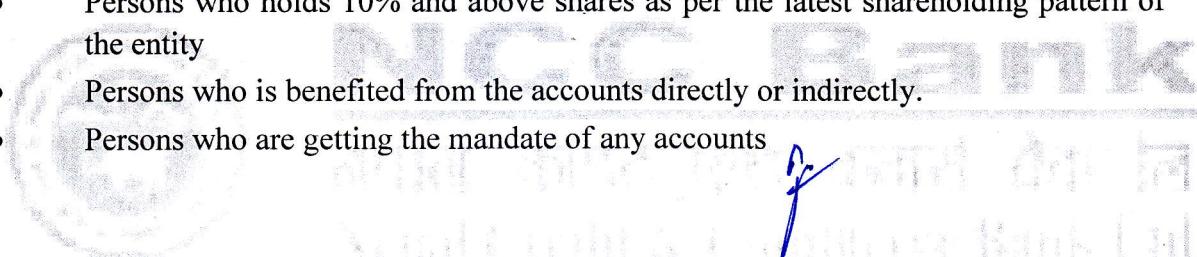
Primarily the database of World Check shall be considered for identifying the PEPs at National or International Level. Bank also maintains the list of domestic PEPs to the best available information.

5. Identification of Beneficial Owner

In compliance with the clause no 4.8 of the Policy, following procedures are laid down for identification of the beneficial owners:-

Following shall be identified as the Beneficial Owner:

- Persons who holds 10% and above shares as per the latest shareholding pattern of the entity
- Persons who is benefited from the accounts directly or indirectly.
- Persons who are getting the mandate of any accounts



KYC, AML/CFT Procedural Guidelines-2018

For Natural Person, beneficial owner is identified either from written mandate or from conduct of the person who acts on behalf of the customer. For example, guardian of minor account, a person using account of the staff working in his company or is his house maid, etc.

For Legal Person

1. Obtain the Shareholding Pattern of the legal entity
2. Get declaration that there is no changes in shareholding pattern that is submitted or mentioned in the MOA or AOA
3. If shareholding pattern can't be obtained then obtain the declaration about the shareholding pattern from the particular customer and beneficial owner. This certification has to be made by Company Secretary or Chief Executive or Managing Director or Chairman of that entity.

CAOU shall screen for the information about the beneficial owner of the accounts and customers in social media i.e. face book.

After identification of the beneficial owner, branches shall follow the below procedures:

1. Verify if s/he is listed in internal PEP list or World Check, if found categorize the account as PEP and high risk. If sanctions, do not open the account.
2. Send the name, address and date of birth of the Beneficial Owner to CAOU for screening if s/he is sanctions or not, if found terminate the relationship with the client by taking the approval from CEO.
3. Duly fill up all the information of the Beneficial Owner in the AML Software.
4. Obtain the following documents of Beneficial Owner
 - o Copy of Citizenship Certificate. If citizenship couldn't be obtained then obtain valid Driving License or Voters card or ID card issued by Nepal Government Authorities.
 - o In case of entity, obtain the Registration Certificate, License, PAN and Shareholding record. If shareholding not available, declaration of shareholding pattern. Get all the copy attested by the account holder if not produced the original copy.
 - o Contact Number of the Customer.
 - o Contact Address
 - o Fathers Name or Mothers Name
 - o Occupation Details
 - o Photograph

5. CDD for Safe Deposit Lockers:

The CDD assessment for Safe Deposit Lockers will be same as Account Opening procedures under Personal Account 'SDD' or 'ECDD'. However, the concerned branch must ensure that CDD assessment has been completed before renting out Lockers.

6. Record Maintenance of Beneficial Owner:

KYC information of beneficial owner must be digitalized and should be made available to examine and analyze when required and ask by regulatory.

The customer and beneficial owner's identification including the periodic updates must be incorporated as the primary work plan of the bank.

6. Risk Categorization of the Customers

- a) In compliance with 4.7 of the AML/CFT and policy 2018 of the bank, loan clients shall be classified based up on the limit as below:-

Personal Loans Limit	Institutional Loans Limit	Risk Grade
Above 50 Million	Above 150 Million	High Risk
30 Million to 50 Million	100 Million to 150 Million	Medium Risk
Below 30 Million	Below 100 Million	Low Risk

If there is no space to record in Pumori the KYC risk for loan account, classify the account on its operating account like: current account. If current account is also not available, classify on saving or other account with remarks.

- b) As per Clause no 4.9 of the Policy, Indicative List of the customer who should be classified as per the risk grade are:-

High Risk Accounts:

- a. PEP's and Undivided family members, PEP owned Business
- b. Citizens of High Risk Countries and customer dealing as occupation/business locating in High Risk Countries.
- c. Citizens of the countries who are not partially/fully complied with AML/CFT standards
- d. Customer reported under STR/SAR

- e. Non Residential Nepali (NRN)
- f. Non Face to Face Customers (NF2F)
- g. Customers with Dubious Standard
- h. Manufacturing and dealership in weapons and ammunition
- i. Bullion Dealers/Jewelers
- j. Gambling/Gaming related services
- k. NGO/Charity/Trust (that receives donation) excluding promoted by UN
- l. Religious Organizations
- m. Remittance Agents**
- n. Money Changers**
- o. Customer who conducts transactions through electronic means and medium only.
- p. High Net worth Individuals having Annual Average account Balance of NPR 100 million and above. This type of account shall be classified and recorded on CBS on Half Yearly basis.
- q. Individual accounts with annual turnover (Summation of Debit or Credit) of NPR 50 million and above (except loan). This type of account shall be classified and recorded on CBS on Half Yearly basis.
- r. Non Individual Accounts with annual turnover (Summation of Debit or Credit) of 100 million and above (except loan). (Exclude BFIs, Insurance Companies, Public Organization owned by Government etc.). This type of account shall be classified and recorded on CBS on Half Yearly basis.\

Transaction monitoring of ECCD Customer will be done by Compliance Officer regularly and shall be reviewed by Compliance department.

If customer profile needs to be upgraded as High Risk or downgrade risk category, Compliance Officer should complete ECDD form and update customer record accordingly after taking necessary approval from ECDD account opening authority.

It is the duty of every staff of NCC Bank to report suspicious and unusual transactions to the immediate reporting or if deemed necessary to Compliance Department, which will be further reported to FIU as suspicious transaction within three days of reporting by branch/unit. All concerned staff of NCC Bank must know its Customer, including the ultimate beneficial owner (if different from legal owner), its economical background and or its normal activities. It is through knowledge about customer or other "give-away" signs that may arouse staff gut-feelings that a money laundering activity may be taking place.

Medium Risk Accounts:

1. Watch list Customers identified under Transactions Monitoring
2. Business not falling under Low Risk and High Risk.
3. Non-Financial Institutions
4. Pawn brokers
5. Auction Houses
6. Antique Dealers
7. Venture Capital Companies
8. Leasing Companies
9. Investment Companies
10. Foreign exchange brokers and dealers (money service bureaus- MSBs)
11. Stock, Security and Commodity Brokers
12. Individual accounts operated by power of attorney (Mandate) to third parties except family members.
13. High Net worth Individuals having Annual Average account Balance of NPR 70 million and above (**except loan**). This type of account shall be classified and recorded on CBS in Half Yearly basis.
14. Individual Accounts with annual turnover (Summation of Debit or Credit) of NPR 30 million and above (**except loan**). This type of account shall be classified and recorded on CBS in Half Yearly basis.
15. Non Individual accounts with annual turnover (Summation of Debit or Credit) of NPR 70 million and above (**except loan**). (Exclude BFIs, Insurance Companies, Public Organization owned by Government etc.). This type of account shall be classified and recorded in CBS on Half Yearly basis.

Low Risk Accounts

1. Banks/FIs regulated by NRB, Government Department and Government owned companies, Government Corporation and their private companies, local bodies and authorities
2. All deposit and borrower accounts pertaining to the Government of Nepal, Governmental Bodies/Corporations/ Companies/Organizations, JVs with Govt., Regulators, FIs, and statutory bodies
3. Listed public companies in NSE and other organization whose financial statement is publicly available.
4. Salaried employees

(A) 



5. People belonging to lower economic strata of the society whose accounts show small balances and low turnover.
6. I/NGOs promoted by United Nations or its agencies
7. All accounts other than those classified as High Risk and Medium Risk

c. Sanctions Country

Below mentioned countries are under different kind of sanctions imposed by United Nations Security Council (UNSC) States which are further administered by Office of Foreign Asset (OFAC). OFAC may freeze assets of embargoed countries, prohibit payment of funds to individuals and countries on the embargo list, or prohibit provision of services to countries subject to UNSC sanctions. Some sanctions are more restrictive than others, and apply to the whole country, while others are specifically targeted certain individuals or entities within a country. Bank shall not conduct the transaction or establish relationship with the country or to the people of that country. Currently, following countries are included under sanctioned:

- North Korea
- Iran
- Libya
- Ivory Cost
- Central African Republic
- Democratic Republic Of Congo
- Eritrea
- Guinea-Bissau
- Iraq
- Lebanon
- Somalia
- South Sudan
- Sudan
- Yemen

[Handwritten signature]

[Handwritten signatures]

*This is the Indicative List which shall be changed from time to time.

d. High Risk Country

Name of Countries

Egypt
Trinidad & Tobago
Myanmar
Vanuatu
Tunisia
Venezuela
Haiti
Bosnia-Herzegovina
Afghanistan
Syria

NCC Bank

*This is the Indicative List which shall be changed from time to time.

7. Know Your Employee (KYE)

In compliance with 4.10 of the Policy, Human Resource Department shall collect the required information of the staffs and update it from time to time as a part of KYE. HR department shall monitor the staff's transactions regularly. If any deviations are observed between the profile of the staff and their transactions, then may ask for the justification. If any discrepancies are observed then, HR department shall report the STR to Head Compliance. HR department may prescribe the limit of deposit and withdraw in the staff salary accounts.

List of Information for KYE

- Identity (Name & Address)
- Date of Birth
- Family Tree
- Academic/Educational Qualification
- Citizenship
- Professional Background
- Work/Past Employment
- Others as needed

8. Customer Due Diligence:

a) Normal Customer Due Diligence (CDD)

In compliance with clause no 5.3 of the Policy, risk of the customer shall be evaluated by the branches conducting the Normal Customer Due Diligence for Low Risk and Medium Risk as per **Annexure-5**. Low Risk and Medium Risk customers are subjected to CDD as per clause no 5.1 of the Policy.

9. Enhanced Customer Due Diligence (ECDD)

In compliance with the clause no 5.2 of the Policy, Enhanced Customer Due Diligence shall be carried out for High Risk Customer at least once a year as per **Annexure-6**. ECDD is applied to the following customers:-

- 1) High Risk Accounts
- 2) If the customer is Foreigner
- 3) If the customer is from the countries that are not implementing AML / CFT Policies.
- 4) If the customer is listed in the stock exchange of the countries that are not implementing AML / CFT Policies
- 5) If the beneficial owner of any legal person or entity can't be determined publically.
- 6) If the customer is HPP or PEP.
- 7) If the customer is found to be high risk customer or suspicious.

Designated staff at branches and central level shall obtain at least following document/information in addition to normal KYC procedure during conducting ECDD

1. Personal information and identification
2. Occupation or nature of business
3. Purpose of opening account and establishing relationship
4. Expected pattern of activity in the account in terms of transaction types, volume and frequency, approximate annual income with sources of income/wealth, net worth declaration
5. Expected origination and destination of funds
6. Incorporation document and business certificates
7. In case of Politically Exposed Person and High Position Person, identification documents and occupational details of one house family members shall be obtained.

8. Understanding of the customer's customers specially in the case of correspondent banks and foreign entity.
9. Details of the other personal and business relationships the customer maintains
10. Details of other banking relationships the customer maintains including multiple banking declaration in case of borrowers
11. Annual reports, audited financial statements and other reports shall be obtained during the review of customer profile or when required. However, financial audited and tax clearance shall be demanded as per the transaction profile of customer.
12. AML/CFT policies, procedures and controls specially in case of correspondent banks, foreign entity and third party service
13. Local market reputation and image of the person through review of media reports or other means

Designated staff at branches and central level shall follow the below mentioned procedures during Conducting of ECDD

1. Examine the purpose and background of those customers whose financial and legal purpose are not clear despite of being a large entity.
2. Examine the background and purpose of the transactions.
3. Examine the control over the accounts and continuously monitor transactions and confirm for monitoring suspicious activity.
4. Obtain the additional information related to the customer, beneficial owner and related parties.
5. Obtain the additional information related to the professional relation, transactions and their purpose and nature.
6. Cross verify the documents and information obtained from external sources if available.
7. Continuously update the information about the customers.
8. Obtain the source of fund and the asset by obtaining the declaration from the customers.

All branches should ensure maintaining and updating of customer risk profile on a continuous basis. In addition to this, Branches shall maintain the report of customer follow up as per the **Annexure-7** during updating of the KYC, CDD and ECDD.

10. Correspondent Bank and Domestic Bank Relationship

In compliance with the clause no 7 of the Policy, following procedures shall be carried out

- Before establishing the relationship with correspondent bank or being the agent of any entities, approval from CEO shall be obtained.
- Compliance Department's consent shall be obtained for establishing relationship with correspondent Banks and Domestic banks in the perspectives of KYC and AML.
- The Bank's Treasury Department, Corporate office is responsible to conduct CDD for the Bank's existing correspondent banks as and when required and not less than on yearly basis with the information of:
 - Identification and verification of the respondent bank/Agency.
 - Information about the respondent bank's/agencies major business activities.
 - Information about management, nature of business, major business activities, date & place of incorporation, license & certificate of registration, website, address where they are located, information of AML/CFT officer, compliance officer, number of branches etc.
- On the basis of publically available information treasury department must access the prestige of respondent bank/agency, condition of bank/agency regulation and supervision and any action taken for breach of AML/CFT or not.
- Treasury Department to access the AML/CFT measures taken by the respondent bank/agency for prevention and detection of money laundering.
- Treasury Department to obtain confirmation if the respondent bank/agency has the transactions with the shell bank or not.
- Treasury Department should pay special attention when continuing relationships with respondent banks/agency that are located in jurisdictions having poor KYC standards or have been identified as being "non-cooperative" in the fight against money laundering and if found to be non-compliance of AML-CFT measures, then the relationship must be terminated.
- Obtain the Correspondent Banking Questionnaire from the respondent bank/agency at least on yearly basis. Treasury shall obtain the questionnaire filled up from all the respondent bank and domestic banks. Compliance Department may revise the questionnaire as and when required as per the changes in laws and regulation.
- Obtain the Correspondent Banking and Domestic Banks Questionnaire at least on yearly basis as per **Annexure-9**.

11. Threshold Transaction Report (TTR)

As per the clause no 10.1 of the Policy, Following procedures are laid down:-

- AML/CFT unit shall prepare the TTR report being based on the guidelines prescribed by FIU, NRB.
- TTR report thus generated shall be submitted to FIU on weekly basis via Go-AML software and in Compact Disc (CD)
- Deviations between the profile of the customer and conducted Threshold Transactions shall be studied by the branches. If any deviations are observed then branches must notify the AML/CFT unit.
- A copy of the TTR submitted to FIU-Nepal should be available at the Compliance department as a permanent record.
- AML/CFT Unit shall analyze the report sent by the Branches and report to FIU as STR if serious deviations are observed.

Following transactions are considered as Threshold Transaction for the purpose of monitoring:

- Deposit or withdrawal of NPR 1.00 million or more into or out of an account in one transaction or in a series of transactions in one day.
- Inward or outward wire transfer of NPR 1.00 million or more (**in cash**) into or out of an account in one transaction or in a series of transactions in one day
- Exchange of foreign currency equivalent to NPR 0.5 million or more (**in cash**) by a customer in one transaction or in a series of transactions in one day.

Followings transactions are exempted from Threshold Transactions reporting and need not to be reported to FIU. However, such exemption is not applicable for any transaction suspicious for financing of ML/FT activities.

1. Transactions of Government and Government Offices,
2. Transactions of any entity established under any special act,
3. Transactions of Bank with other Bank and Financial Institutions or Government agencies,
4. Transaction executed by public companies with other public companies, government or semi government offices, organization, institutions, companies or entities established under special act.
5. Transaction executed by insurance companies for re-insurance business.
6. Loan and Advances or other facilities provided to customer according to prevailing laws and regulations.
7. Transaction of UN, their offices, and international organization





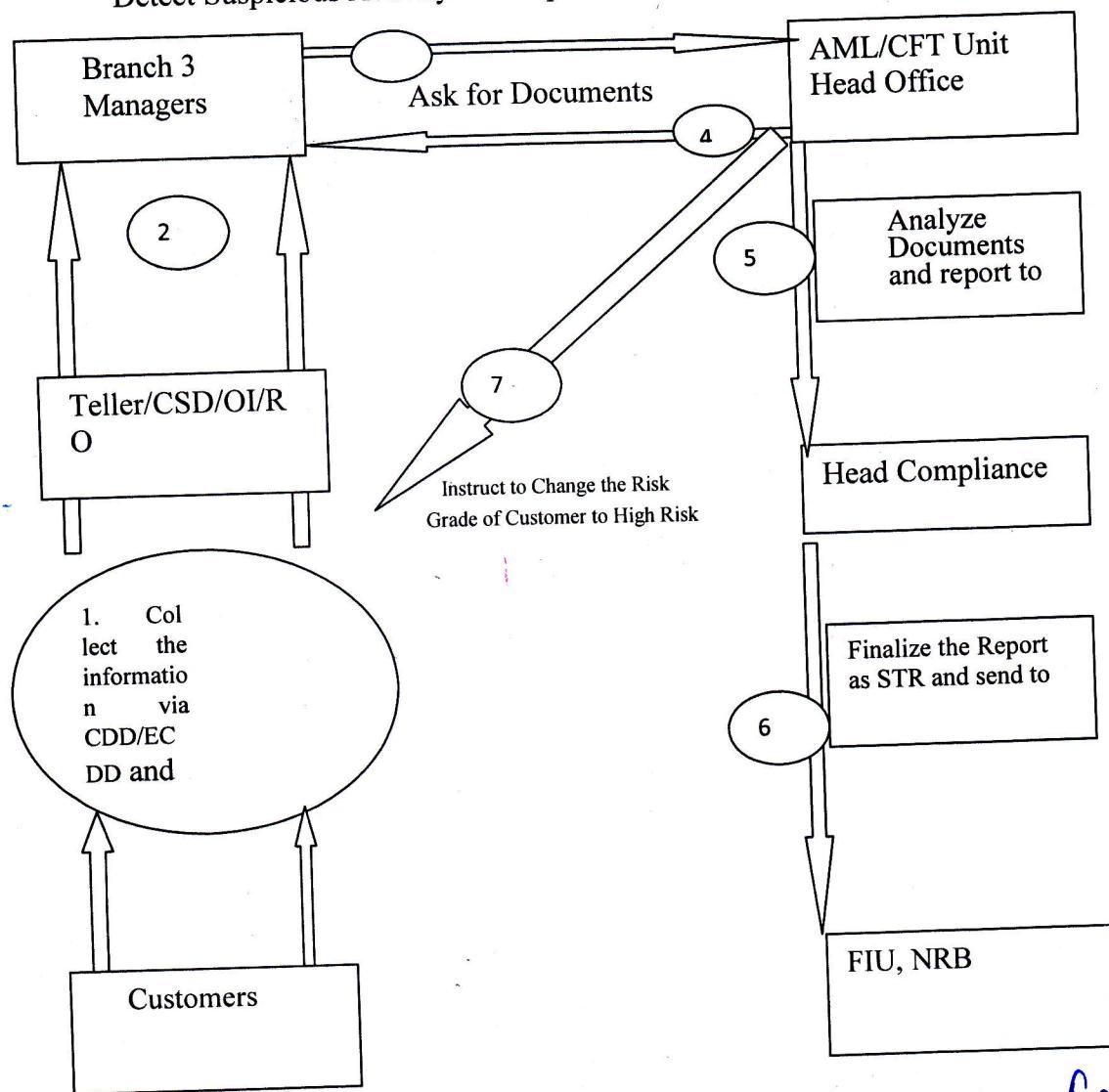
8. Transaction executed for the facilities provided to employee by any bank and financial institutions
9. Amount transfer through cheque (clearing) from one bank to another bank (within Nepal)

12. Suspicious Transaction Report (STR) Procedures

In Compliance with the clause no 10.2 of the AML/CFT and KYC Policy, Bank shall follow the following procedures for detection, reporting and recording of the STR.

STR Mechanism

Detect Suspicious Activity and Report to



1. Staff members designated at the front office shall detect the suspicious behavior of the customer interacting with them and report it immediately to the Operation In charge or Branch Managers.
2. OIs and the Branch Managers shall screen the behavior and the transactions of the customer and analyze the deviations between the profile and their transactions.
3. If any huge or complex deviations are observed, then reports to the Head Office Compliance Department as suspicious pattern/Activity report it immediately as per the **Annexure-8**.
4. Compliance Department shall further analyze the report and ask for the necessary documents with the Branches.
5. Head Compliance shall decide if the transactions are STR or not. And report it to FIU within 3 days from the date of confirmation.
6. Compliance Department shall instruct the Branches for changing the Risk grade of the Customer to High Risk Grade after reporting STR.
7. Head Compliance/Compliance Officer shall maintain the record of STR.

Designated staffs at the Bank shall follow the guidelines issued by Financial Information Unit Nepal for determining the suspicious characteristics of the transactions in the customer account.

Some of the types of transactions that provide the ground of suspicious transaction are:-

- Cash transactions conducted in an unusual amount in the account
- If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate
- Minor Accounts with abnormally large transactions
- Huge transactions in the Account of Housewives, Student, Doctor, Lawyer, Government Officers
- If multiple mandates are provided for the account
- If same person getting mandate on various accounts
- Accounts receiving the foreign donations frequently
- Transactions having no conformity with the initial purpose of account opening
- Transactions having no relationship with the business of the customer
- If the customer declares that the remittance is sent from abroad but the remittance system shows that the remittance is received from Nepal.

- 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.
- If anyone unnecessarily clarifies or tries to clarify legality of amount or transaction.
- If customer-conducting transaction looks confused, nervous, hurried, or wants to remain reserved at the time of transaction.
- If it is evident that the asset is earned from any offence against or abuse of children, women or destitute or any other individual.
- If transaction seems to be reported based on the news or commentary published in national or international news media about any individual or organization.
- If same address or telephone number/mobile number is provided for different unrelated customers accounts.
- If any customer shows unnecessary interest in suspicious transaction or makes unnecessary and unnatural queries about the internal management of such transaction.
- If person sending money cannot provide even general information about the recipient of money.
- If a small capital holder tries to transfer or receive unreasonably huge amount.
- If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.
- Gives rise to reasonable ground of suspicion that it may involve the proceeds of crime.
- Appears to have no economic rationale or purpose.
- Providing misleading information /information not easily verifiable while opening an account.
- Large cash withdrawals from inactive accounts.
- Sudden increase in cash deposits of an individual with no justification.
- Large cash deposits in same account.
- Receipt and payment of large cash sums with no obvious purpose to account holder/businesses.

13. Wire Transfer Procedures

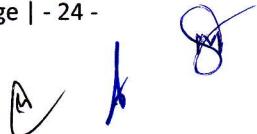
As per the provision mentioned in the clause no 10.3 of the Policy, following procedures are laid down that are applicable on all remit based transactions, inward fund transfer through SWIFT and outward fund transfer through SWIFT.

1. Confirm and ensure the originator or sender's Name, Address, Account Number,





- Customer Identification Number. If account number is not available, identify the transaction number.
2. Confirm and ensure the beneficiary's name, address and account number. If account number is not available, identify the transaction number.
 3. All the SWIFT transfers (Inward/Outward) are screened through SWIFT screening for controlling sanctioned parties.
 4. If SWIFT screening is not available or not functioning, it has to be checked through the designed module of screening of sanctions parties or PEPs manually before sending the fund or receiving the fund of non account holders.
 5. The reliability, reasonability and consistency should be assessment on the amount received through wire transfer. If the amount is high and suspected as not having consistent with the customer profiles, it has to be assessed in detail before crediting to the account or paying out.
 6. If the sanctions screening, suspicious transactions and customer behavior shows indications of mis match, it has to be referred to Compliance Department before executing the transactions. Concerned functional department/unit should not execute transaction under above circumstances.
 7. In case of remittance payment of various remit companies, the remit company must have inbuilt Sanctions Screening mechanism mandatorily. Bank shall not deal with that remit companies who do not have such sanctions screening mechanism on software.
 8. If the beneficiary is not the account holder, his/her valid Identity, Address and Contact number should be taken at minimum.
 9. Transaction should not be executed of those persons (both Beneficiary and Originator) who are under the sanctioned list.
 10. It is most important for recording the wire transfer transactions irrespective of their amount and nature. Concerned staff working on SWIFT and Remit operations shall prepare the record of Inward wire transfer. The record should be maintained on secured way. The primary format of the transaction



S.NO.	Originator Name	Account Number of Originator/Trans Number	Address of originator/ or DOB/or place of birth or citizenship Number	Beneficiary Name	Account Number of Beneficiary /Trans Number	FCY currency	FCY Value	LCY Amount	purpose /remittance information

Recorded should be in the following form on daily basis:

- If information as mentioned above is not available and the amount is exceeding Rs 75,000 NPR, the transaction should be suspended. Should not execute for both outward and inward wire transfer.
 - The information should compulsorily be in the payment message of each remit. Remittance transaction should not be executed if anyone information is lacking. In case of exceptional situations, COO's approval should be taken for payments. COO should give approval on the ground that the transaction is genuine in nature and information can be taken later on. That kind of exceptional practices should be avoided to the best possible.
 - Above mentioned report on the given table should be prepared on daily basis by SWIFT Operations and Remittance. It has to be secured stored. One copy should be reported to Compliance Department on daily basis.
11. Compliance Department regularly monitors the wire transfer transaction on very next day on the AML and CFT perspective.
12. From Risk Assessment and Risk Management perspectives, the wire transactions exceeding the amount USD 1.00 Lac or equivalent, compliance department's consent should be taken. SWIFT Operations or Remittance should send the detail on the given format and Compliance Department send consent though E-Mail for the payment of such transaction.
13. Monitoring of the wire transfer transactions shall be conducted on regular basis by Compliance Department. Compliance department assess the overall risk on the wire transfer transaction and suggest for future precautions.




14. If the beneficiary is not the account holder, his/her valid Identity,Address and Contact number should be taken at minimum.
15. Bank should take information through questionnaire from the remit companies regarding the compliance of KYC, AML and CFT as per the requirements of the Bank.

Training and Development

As per the Clause no 16 and 17 of the Policy, following procedures are laid down for training and development.

1. Training of KYC, AML and CFT shall be a part of HR Department's annual training plan. Compliance department provides the topics and tentative annual schedule of internal training program for a year.
2. Human Resource Department shall provide the list of staffs provided training on AML/CFT for record and compliance purpose.
3. Compliance Department shall design and recommend the content of orientation program which shall include importance of AML/CFT & KYC, staffs responsibility to detect and prevent Money Laundering and combating Financing of Terrorism and the basic requirements at the Bank.
4. Bank shall send the staff members in the national and international training on AML/CFT & KYC as per requirement.
5. Compliance Department shall prepare annual plan for AML/CFT training after conducting the need assessment of the staff members, refresher training to senior management, group of customers, shareholders holding 2% and above and other stakeholders of the Bank before starting of the Fiscal Year.
6. Head of Compliance Shall conduct the online test for all the staffs at least twice in a year on AML/CFT. All the staff members must participate in the test.

CAOU follows the procedures as below on account approval and further diligences.

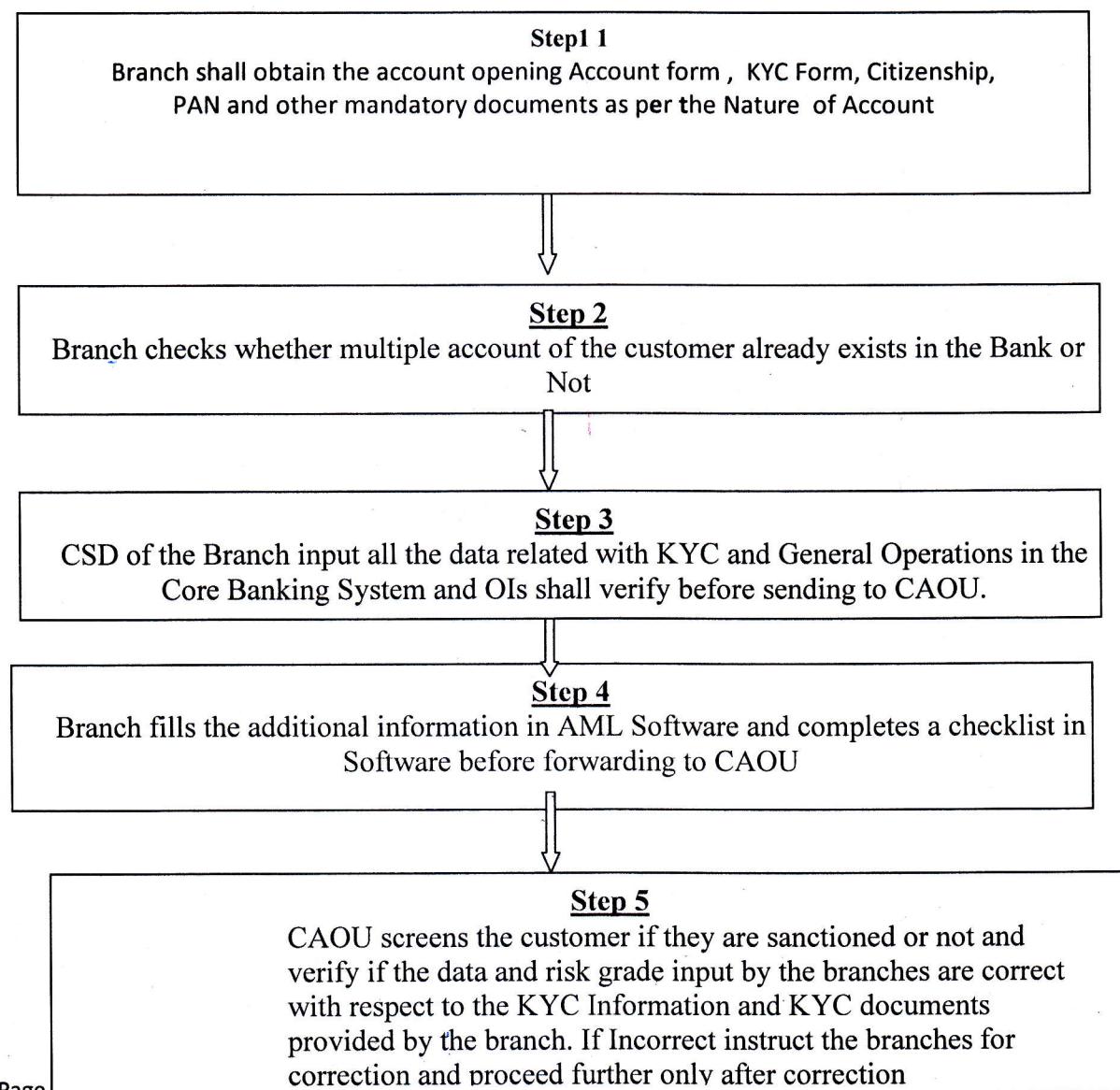
Work Scopes and objectives

- a) Compliance of bank's KYC, AML/CFT Policy, NRB Directives, Anti Money Laundering Act and Anti Money Laundering Regulations of Nepal Government.
- b) Ensure that branch has properly identified the customer through Customer Acceptance Procedures and Customer Identification Procedures of the Ban
- c) Ensure that account opening form are duly filled up in compliance of KYC norms

KYC, AML/CFT Procedural Guidelines-2018

- d) Ensure that information are updated on CBS in regard of KYC information as required by NRB Directives and Bank's KYC, AML/CFT Policy and Procedures
- e) Check whether the account falls under the scopes of suspicious background or under sanctions criteria/list
Monitor the accounts which are approved on the pending documents and update the status periodically
- g) Prepare report periodically as per the Bank's MIS Guidelines and its own need.
- h) Check and get executed that branches follow the procedures and practices as given in the Policy and Procedures regarding the KYC and AML.
- i) Make aware the branches about the lapse and problems faced during the account opening procedures due to operational lapses in branches and CAOU itself.
- j) Advise the management for needful changes and improvements in the current practices when needed.

Procedures of Account Opening/Approval





Step 6

Approving authority at CAOU must approve the accounts both in CBS and AML Software only after verifying that the account are undergone through all the above steps.

Documents and information to be verified

CAOU must obtain the following documents while approving the accounts.

- Account Opening form (signed by at least OI)
- Additional KYC Form
- Copy of Citizennships
- Copy of Registrations
- PAN
- Tax Clearance or Tax Submission Form
- Picture/Photo Image
- Audit Report (Covering reporting of auditor)
- Other documents as needed to the CAOU

Once the new account are opened, all the operational functions like signature upload, change of signature, photo upload , thumb impressions uploads , occupation, Address, Annual Turnover, and other KYC update functions etc on CBS and on relevant documents shall be carried out/approved by the branches itself. But, the change in Name of the Account must be approved from CAOU on branch recommendation.

14. Record retention in digital form

Branches shall keep the record of the documents related to the identification of the customer, beneficial owner in the both hard copy and the digital form. The checklist of the documents that are in customer account opening shall be kept in the AML Software. CAOU also maintains the documents sent by the branches for account opening in digital form. A archiving system shall be developed for storing the documents on electronic form by branches and CAOU.

15. Electronic Transactions Monitoring Procedure

AML Software in Transactions Monitoring

In compliance with the clause no 10 of the Policy, compliance department shall monitor the transactions of the customer on regular basis.

Following types of the transactions shall be screened by Compliance Department on regular basis:-

1. Monitoring of all incoming and outgoing wire transfer on daily basis.

Compliance Department shall monitor all the incoming and outgoing Wire transfer on daily basis. For wire transfer transactions that seem to be of unusual pattern compliance department ask for the documents with the branch and analyze them. If any Suspicious is observed, then report as STR to FIU-Nepal.

2. Monitoring of the electronic transactions

Compliance Department shall monitor the transactions that are taking place electronically. Such transactions are conducted through Mobile Banking, Internet Banking and eSewa. If any Suspicious is observed, then report as STR to FIU-Nepal.

3. Monitoring of the transactions taking place in the account of the High Risk customers.

The report of transactions take place in the account of the High Risk customer is provided by the AML Software on daily basis. Compliance Department shall monitor it on daily basis. If any Suspicious is observed, then report as STR to FIU-Nepal.

4. Monitoring of the card transactions.

Compliance Department shall study the transactions conducted by using the card in the ATM either within the country or outside the country. Compliance department shall ask for the documents that justifies the transactions with the Branch. If any Suspicious is observed, then report as STR to NRB, FIU.

5. Monitoring of the transactions being based on the frequency and amount.

Compliance Department shall analyze the report being based on the high Frequency and High Volume, Unusual cash transactions, transactions being taken in the staffs

account. These reports are generated from the AML Software on daily basis. If any Suspicious is observed, then report as STR to NRB, FIU.

6. Monitoring of Adverse Media.

Compliance Department shall monitor the adverse media news on daily basis. Monitoring of the adverse media shall include any two online media of Nepal and any two national daily newspapers. The adverse media news must be related to Tax evasion, Crime, Corruption, Frauds, Forgery, Money Laundering etc. It does not fall the information like: loan default, recovery notices etc.

Compliance department screens the name identified on media monitoring in the central data base. If name matches, then compliance department forward it to the concerned branches for further verification. If branch confirm as the same person, then compliance proceeds for further course of actions and if it is not matched or different person, then compliance department close the issue.

All the persons identified on media monitoring should be recorded in a register by the compliance. Those data base should be further updated with the branch level status and further course of action taken.

Maintenance of Database

In compliance with the Clause No 14 of the Policy, Compliance Department shall maintain the internal database of PEPs, High Ranking Officials, Influential Persons as per **Annexure-10** and Database of the letters received form Authority as per **Annexure-11**.

Risk Assessment:

AML/CFT Unit must prepare and submit Quarterly AML Progress Report and annual AML/CFT Risk Assessment of the Bank to Financial Information Unit within the 15 days of first quarter.

16. Updating KYC, Conducting CDD, ECDD

Step 1

Branch shall conduct the KYC, CDD and ECDD as per the nature of account



Step 2

CSD of the Branch shall obtain all the mandatory documents and input all the data in the Core Banking System



Step 3

BM/OIs must verify if the all the data are correctly inputted in the CBS or not and approved as per the operational authority level

17. GO-AML Software:

The Go-AML application is a fully integrated software solution developed specifically for use by Financial Intelligence Units (FIU's) and is one of UNODC's strategic responses to financial crime, including money-laundering and terrorist financing. It is an electronic reporting system which developed for receiving, processing and analyzing reports made by financial institutions or other entities according to the requirements of domestic anti-money laundering laws and regulations.

As per the regulatory requirement bank shall start to report Threshold Transaction and Suspicious Transaction electronically through Go AML Reporting system from 1st Kartik 2075.

18. Trade Based Money Laundering:

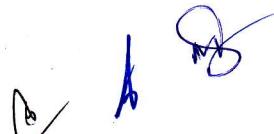
A. Trade Related CDD Requirement:

Knowing customers is a key part of the controls required to mitigate trade-based money laundering risks. CDD is particularly important for Bank to manage and monitor the risks associated with customers on an ongoing basis throughout the relationship.

Key customer information related to trade-based activities that is collected may include, but is not limited to, the customer's:

- (a) Business nature, such as major products, jurisdictions and markets;
- (b) Delivery / transportation mode for goods or services;
- (c) Major suppliers and buyers;
- (d) Products and services to be utilized from;
- (e) Anticipated account activities;
- (f) Anticipated major methods and terms of payment and settlement;
- (g) Internal customer risk assessment ratings.
- (h) Other information from the relationship manager or other relevant staff.
- (I) Reviewing trade finance documents, for example, bills of lading and commercial invoices;
- (j) Conducting company verifications and media searches;
- (k) Conducting client account activity reviews;

- Where irregularity regarding customer's trade-related activities is identified at any stage, bank should consider obtaining further information to assess whether there may be a legitimate explanation to calm the concern. A situation that constitutes an anomaly may not necessarily give rise to, or elevate, the risk of trade-based money laundering. In particular, if there is a legitimate explanation for the anomaly, there may be no such risk implications.



f

- Bank should ensure proper documentation and record keeping of both the initial CDD assessment and any updated information and explanations. This should include customer information, any decisions made, and any rationale for a decision.

B. Trade Related Transaction Monitoring:

The purpose of transaction monitoring is to alert activities which appear to be unusual or suspicious for further examination and investigation.

If trade finance unit found any trade related transactions to be suspicious, it is responsibility of unit to report suspicious activities to compliance department.

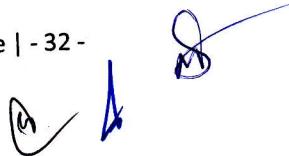
Typical Trade Based Money Laundering Typologies:

1. Over Invoicing or Under Invoicing
2. Over Shipping or Short Shipping
3. Fictitious Trade
4. Use of Shell or Fictitious Companies
5. Multiple invoicing of goods and services
6. Black Market Trade

C. Screening Techniques:

- Identifying and screening all relevant parties to a transaction and other information contained within trade documents against applicable sanctions lists.
- Screening for and recording in relevant systems information on all relevant fields to a transaction.

- Counterparty name(s) and location(s)
- Counterparty bank(s), their capacity in the transaction, and location(s)
- Customer name(s) including individuals and companies
- Carrier / charter / agent
- Country of origin
- Description of goods / commodities
- Freight forwarders and shipping companies
- Originating and recipient entities of the goods (i.e importer and exporter)
- Shipper, consignee and notification party on transport documents
- Shipping route (such as the port of loading, port of discharge, port of transshipment)
- Vessel name(s)
- Flag of vessel



f

D. Red Flags:

1. Customer Red Flag:

- (a) Uncommon transaction structure or overly complex transaction structure without a clear and legitimate commercial purpose or some reasonable justification.
- (b) The transaction is not commensurate with known customer profile, structure or business strategy. In a trade-based money laundering context, this may be where the nature or type of goods shipped is not in line with the business nature of the customer (e.g. a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals), the customer has no experience in the goods in question, or the size or frequency of the shipments appear inconsistent with the scale of the customer's regular business activities (e.g. a sudden surge in transaction size).
- (c) The customer significantly deviates from their historical pattern of trade activity (i.e. in terms of value, frequency or merchandise) with dubious pricing of goods and services.
- (d) The customer or parties have suspicious addresses. For example different transacting businesses may share the same address or the businesses only provide a registered agent's address.
- (e) The customer reacts aggressively to know your customer questions or tries to force the bank to take CDD shortcuts by citing time pressures.
- (f) The customer refuses any form of contact or communication with the bank, without a valid reason for that refusal.
- (g) The customer is overly keen to waive discrepancies.
- (h) The customer offers to pay unusually high fees to the bank.

2. Documentary Red Flag:

- (a) The shipment locations of the goods, shipping terms, or descriptions of the goods are inconsistent with the L/C. This may include changes in shipment locations to high risk countries or changes in the quality of the goods shipped.
- (b) Significant discrepancies appear between the descriptions of the goods on the bill of lading (or invoice) and the actual goods shipped.
- (c) There are substantial discrepancies in merchandise descriptions, e.g. quantities, weights.
- (d) Obvious over or under pricing of goods (that is, significant discrepancies appear between the value of the goods reported on the invoice and the known fair market value of the goods). In a trade context, where goods are highly overvalued, the importer could be moving funds out of their country. Conversely, where the goods are highly undervalued, the exporter could be moving funds out of its country.
- (e) Obvious misrepresentation of the quantity of goods shipped. The contract value is unusually high for a party.

[Signature]

[Handwritten signatures]

- (f) Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.
- (g) The transaction involves the use of repeatedly amended or frequently extended L/C.
- (h) The documents show excessively amended terms.
- (i) The documents contain non-standard clauses or phrases or have other unusual characteristics.
- (j) There are dubious unauthorized alterations or amendments to the documents.
- (k) The beneficiary or applicant refuses to provide documents to prove shipment of goods (indicates possible phantom shipping or multiple invoicing).
- (l) There are other dubious indicators such as unusual codes, markings or stamps on the monetary instruments (e.g. drafts or bills of exchange, or future dated bills of lading, and transaction under L/C without proper transport document or document evidencing shipment / delivery of goods).
- (m) There are indications that the descriptions of the goods are coded or disguised.
- (n) The customer requests an L/C without calling for a transport documents or documents evidencing shipment or delivery of goods; or an amendment to a L/C removing the transport document or document evidencing shipment or delivery of goods as required in the original terms.
- (o) The transaction is without transport documents evidencing movement of goods.
- (p) The bill of lading describes containerized cargo but without container numbers or with sequential container numbers.
- (q) There are indications that documents have been re-used.
- (r) There are indications of double invoicing.
- (s) The invoice shows "Other/Undefined" charges as an unreasonably high percentage of total transaction value.
- (t) A documentary credit if overdrawn by more than an unreasonably high percentage of the original value
- (u) The goods in respect of a documentary credit are over shipped by an unreasonably high percentage of the original quantity.
- (v) An L/C is dated later than its date of presentation.
- (w) The description of goods on the transport documents (if any) cannot be linked to the document terms and / or the actual invoice.
- (x) The customer re-submits a document rejected earlier as a result of financial crime risk concerns.
- (y) The non-negotiable bill of lading is consigned 'to be advised between applicant and beneficiary' (consignment should be to a named party).
- (z) The customer makes a trade-related claim on a stand-by L/C before or a short period of time after its issuance.

18

AM

3. Transaction Red Flag:

- (a) The transaction structure is designed to conceal information or make it difficult for Bank to obtain certain information or the true nature of the transaction. This may include indications that a shipment is structured to disguise proliferation risks.
- (b) The transaction involves round-tripping or circular transactions.
- (c) The transaction involves an uncommon or complicated movement of goods and/or third parties without an obvious purpose.
- (d) The method of payment appears inconsistent with the risk characteristics of the transaction.
- (e) The shipment does not make economic sense, takes an uneconomical shipping route, or the shipping route is unclear.
- (f) The mode or method of shipping is unclear.
- (g) The customer has unusually frequent round transactions.
- (h) The transaction involves the use of front or shell companies without a clear and legitimate commercial purpose or some reasonable justification.
- (i) The transaction involves sanctioned entities.
- (j) The transaction route involves high-risk jurisdictions or the trade transaction otherwise involves high risk jurisdictions.
- (k) The commodity is trans-shipped through one or more jurisdictions for no apparent economic or other logistical reason.
- (l) The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction, or other indications of possible black market peso exchange arrangements.
- (m) The transaction involves an unusually high number of intermediaries, too many or unnecessary parties, or transferable letters of credit.
- (n) The tenor of a relevant transaction is not in line with the nature of the underlying commodity financed – for example, in relation to a perishable good.
- (o) Documents such as an L/C received through unverified channels such as unauthenticated SWIFT message.

4. Commodity Red Flags:

- (a) The type of commodity being shipped is designated as “high risk” for trade-based money laundering activities (e.g. precious metals and stones).
- (b) The type of commodity being shipped appears inconsistent with the exporter or importer’s regular business activities.
- (c) The commodity is shipped to (or from) a jurisdiction designated as “high risk” for ML/TF activities.
- (d) Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity’s fair market value.
- (e) The commodity includes dual-use goods.



19. Implementation, Review and Amendments

1. This Procedural Framework will be effective upon the approval of Chief Executive Officer (CEO).
2. Compliance Department shall review and update this AML Procedural Framework annually.
3. Head of compliance may changes the formats given on Annexure on practical and need basis maintain the true spirit of compliance and uses.

Annexure-1: Refusal of Account Opening Form

S. No	Name of the Customer	Legal Id Number	Fathers Name	Purposed Deposit Amount	Refused by	Reason For Refusing account

Prepared By: -

Date: -

Approved By:-

Date: -

Annexure-2: Commitment for Account Opening Form

S.N	Branch	A/C Num	A/C Name	A/C Type	Open Date	List of Pending Docs	Due Date	Committed By	Staff Name (CAOU)	Follow Up	Status




Annexure-3: Approval for Personal High Risk Accounts

High Risk Customer (ECDD) Approval Format

Personal Account:

Branch Name:

<u>Name of Customer:</u>	
<u>Reason for considering High Risk:</u>	
<u>List of Obtained Documents:</u>	
<u>Brief Background of Customer:</u> (Professional Status/Residence/Public position/Details of Business)	
<u>Source of Income:</u>	
<u>Expected Annual Turnover:</u>	
<u>Relationship/Association with any other business (if any):</u>	
<u>Purpose of Account Opening:</u>	
<u>Name list of one house family members:</u>	
<u>Account of one house family member in NCC Bank (if any):</u>	

Hence, recommended to categorize the risk status to High Risk.

Recommended by**Recommended by****Approved by****OR**.....
Branch
Manager.....
Chief Operating Officer.....
Head-Compliance

Annexure-4: Approval for Non-Personal High Risk Accounts

<u>Non-Personal Account:</u>	<u>Branch Name:</u>
<u>Name of Legal Person:</u>	
<u>Reason for considering High Risk:</u>	
<u>List of Obtained Documents:</u>	
<u>Relationship with us prior to this Business deal:</u>	
<u>Brief Background of Customer:</u> Owner/Signatory/Account Operator	
<u>Business Type:</u> Whole seller/Retailer	
<u>How Long Business into Operation:</u>	
<u>Physical presence of business:</u>	
<u>Key person of business:</u> Involvement in any other business (if any)	
<u>Details of Business Outlets:</u>	
<u>Other relevant information</u> that may help approving authority to understand customer and inherent risk.	

Hence, recommended to categorize the risk status to High Risk.

Recommended by

Approved by

Approved by

OR

.....
Branch
Manager

.....
Chief Operating Officer

.....
Head-Compliance

[Signature]

[Handwritten signatures]

Annexure-5: Customer Due Diligence (CDD) Form

CUSTOMER DUE DILIGENCE REVIEW												Recent PP size Photo(co mpulsary) D a t e		
Account Number														
													Account Opened Date:	
Present Address:						Permanent Address:								
Contact No.			Citizenship Nos.			Issuing Office & date:								
Father Name:			Grand Father Name:			Husband/ Wife Name:								
													Remarks, if any:-	
Address verifying supporting documents obtained?						<input type="checkbox"/> Y es	<input type="checkbox"/> N o							
Punished in the Criminal activity in the past?						<input type="checkbox"/> Y es	<input type="checkbox"/> N o							
Mandate to operate the account given to Third Party?						<input type="checkbox"/> Y es	<input type="checkbox"/> N o	<input type="checkbox"/> N o						
Identification of Third Party Signatory obtained?						<input type="checkbox"/> Y es	<input type="checkbox"/> N o	<input type="checkbox"/> N o						
Residential Address of Third Party Signatory verified?						<input type="checkbox"/> Y es	<input type="checkbox"/> N o	<input type="checkbox"/> N o						
Relationship with the Third Party established?						<input type="checkbox"/> Y es	<input type="checkbox"/> N o	<input type="checkbox"/> N o						
HPP/PEP/NF2F?						<input type="checkbox"/> Y es	<input type="checkbox"/> N o	<input type="checkbox"/> N o						
Monthly Turnover:			<input type="checkbox"/> Less Than 5 Lakhs			<input type="checkbox"/> Less Than 10 Lakhs			<input type="checkbox"/> Above 10 Lakhs					
Monthly Transaction:			<input type="checkbox"/> Less Than 15			<input type="checkbox"/> Less Than 25 Lakhs			<input type="checkbox"/> Above 25					
Purpose of Account:		<input type="checkbox"/> Remittanc e	<input type="checkbox"/> savings	<input type="checkbox"/> Business										
Source Of Fund:		<input type="checkbox"/> Salary	<input type="checkbox"/> Remittance	<input type="checkbox"/> Investment										




KYC, AML/CFT Procedural Guidelines-2018

<input type="checkbox"/> Donation	<input type="checkbox"/> Borrowings	<input type="checkbox"/> Loan Repayment	<input type="checkbox"/> Others
		A m o u n t R s	L a k h s
Account Turnover in Last Six Months: Any other remark of account holder noted?		Nos. of TXN	
		H i g h R i s k	Medium Risk
As per the points mentioned above, recommended categorization of account:		<input type="checkbox"/> Low Risk	
Name listed in OFAC (Office of Foreign Assets Control)?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Reason for Recommendation:-		Information Update in Core Banking System: Y <input type="checkbox"/> e <input type="checkbox"/> s N <input type="checkbox"/> o Date Updated on: _____	
Branch Manager Date: _____		CSD Staff Date	

Annexure-6: Enhanced Customer Due Diligence (ECDD) Form

Branch Name:

In Compliance with NRB Directive No. 19.6 and AML Act, sec 7^(a), ECDD has been conducted on the High Risk account as below:

Customer Name:

Deposit Type	Main Code	Total DR Trans. No	Total CR Trans. No	DR Transaction Amt	CR Transaction Amt	Remarks, If any on Trans




KYC, AML/CFT Procedural Guidelines-2018

Update as Yes or No and Remarks on the following information:

S N o	Information	Y e s	N o	Remarks
1	Are income sources disclosed by 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 convenience with client dealing and nature of transactions			
6	Is client or its transactions notified or observed as suspicious			
7	Does Branch conduct ongoing transactions monitoring of customer			
8	Are the frequencies of transactions justifiable			
9	Is customer made amount transfer from one account to another frequently with the aim of concealing/ layering the transaction			
10	Is the customer conducted transaction below threshold limit (8 to 9.99 lakh a day) regularly with the aim of escaping from TTR			
11	Have the customer documents updated like: registration, audited financials, license etc are updated up to this year			

Remarks, If any:-

CSD Staff/In charge

Prepared By

Operation In-charge

Reviewed & Supported by

Branch Manager

Approved by



Annexure-7: Customer Follow-up Form

Account Number	Account Name	Follow up made by Name:	Medium used for follow up	Number of Follow up made

Prepared By:-

Date:-

Approved By:-

Date:-

Annexure-8: Suspicious Transaction Report Form (For Branches)

Date:

To: Compliance Department, Tinkune Kathmandu

REPORTING				
Name				
Position	Branch/ Dept			
Customer Name	Nationality			
Telephone No.	Address			
Occupation	Address / Tel No			
Employer's Name				
Account Number	Account Type	Available Balance Date	Other account (if any)	
NATURE OF TRANSACTION				
-Transaction in Dormant Account remittances		Large/unusual inward/outward		
- Large/unusual cash deposits/withdrawals		Unusual ATM Card withdrawal		
- Activity inconsistent with customer		Other(Specify):		
DETAILS OF TRANSACTIONS TOUCHING SUSPICION				
Amount (Dr)	Amount (Cr) incoming	Details of Remitting Bank (funds) /		

[Handwritten signatures/initials]

[Signature]

KYC, AML/CFT Procedural Guidelines-2018

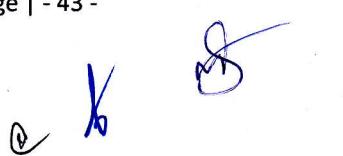
		Destination (outgoing funds)
REASONS FOR SUSPICION		
REASONS GIVEN BY CUSTOMER FOR TRANSACTIONS/ON MAKING FURTHER ENQUIRIES		
OTHER RELEVANT INFORMATION		
IMPORTANT: Please attach copies of (1) Account Opening form (2) Recent account history (3) Suspicious transaction documents AND (4) Customer identification documents. NOTE: You should not inform customer/client of your suspicion.		

REPORTER'S SIGNATURE

Annexure-9: KYC/AML/CFT Correspondence Questionnaire

**PART A : IDENTIFICATION
OF CUSTOMER**

1	Legal Name: (Name of Entity)	
2	Registration Number:	
3	Authority of Registration:	
4	Country of Registration:	
5	Date of Incorporation	
6	Type of license and Number:	
7	License Issue Date:	
8	Authority Issuing license:	
9	Name of Regulatory Authority	
10	Registered Address	
11	Head Office/Corporate Office Address	
12	Phone Number/ Fax Number	



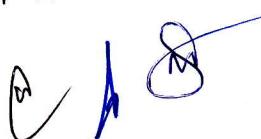
Handwritten signatures and initials are present at the bottom left of the page, including a large 'J' and a smaller 'S'.

KYC, AML/CFT Procedural Guidelines-2018

13	Website		
14	Tax Registration Number		
15	SWIFT Code		
16	Number of Branches	Local:	Foreign:
17	Number of Staffs Working in AML/CFT		
18	Type of Institution		
19	Nature Of Core Business		

PART B : OWNERSHIP AND MANAGEMENT STRUCTURE

20	Legal Identity of Entity	Privately Owned	Publicly Owned	State Owned
21	Share Holding Structure (%)	Promoter: Public:		
22	Name of Primary Stock Exchange and Country			
23	Beneficiary Owners	Does any company or government agency owns or control, Directly and or indirectly 10% or more of share or stakes. if, yes please provide a list of company(ies), and attachment if required. Does any natural person control or own directly and/or indirectly 10% or		J



KYC, AML/CFT Procedural Guidelines-2018

		more of the shares or exercise ultimate control over the management of the entity?				
		If yes, please provide a list of the ultimate beneficial owners, and attachment if required.				
24.	Details of the Board of Directors					
	Name	Address	Nationality	Date of Birth	Position	Brief profile
25.	Details of senior/Executive Management					
	Name	Address	Nationality	Date of Birth	Position	Brief profile
26.	Does any of the Board of Directors or Senior Management belong to PEP (Politically Exposed Person) of your jurisdiction.					
	If Yes, provide details of such persons, add attachment if required					

**PART C : COMPLIANCE GENERAL
AML POLICIES,
PRACTICES AND PROCEDURES**

2	Has the entity's country of registration law designed to	
7		

A ✓ M ✓ J

KYC, AML/CFT Procedural Guidelines-2018

.	prevent money laundering and terrorist financing and is your institution fully compliant with such law?			
2 8 . .	is the entity's country of origin a member of financial task force (FATF) or regional bodies?			
2 9 . .	What is the name of the financial information unit/government body?			
3 0 . .	Does the entity have policies and procedure for AML/CFT? If yes, mention the date of implementation:			
3 1 . .	Does the entity's AML policy meet the requirements of national and international laws and regulation?			
3 2 . .	Does the institution have legal and regulatory compliance program that includes a designated officers that is responsible for coordinating and overseeing the AML framework?			
3 3 . .	Does the entity reviews such policy and procedure? If yes, what is the frequency such review? Mention the latest review date:			
3 4 . .	what is the current AML transaction monitoring process of the entity? If automated, mentioned the name of the vendor/developer of the software. If manual/ others, please mention the procedure in brief.	Automated	Manuals	Others
3 5 . .	is the AML/Sanction policy (policies) subject to approval by your Board or seniors management?			
3	Does the entity documented			




KYC, AML/CFT Procedural Guidelines-2018

6	policy of Anti-Bribery and corruption?		
3 7	Does the entity retain the information and documents related to KYC and AML/CFT, including STR/SARs as required by the law of land?		
3 8	Does the entity's KYC/AML policy incorporate the given information?	<ul style="list-style-type: none"> • Customers identification procedure. • Customers Acceptance policy • Customers Due Diligence ECDD • Transaction monitoring • Record keeping/Retention • Reporting • Procedure on wire transfer • Risk management. 	
3 9	Are the entity's AML Policies and practices being applied to all branches and subsidiaries of the entity both in home country and in international market?		
4 0	In addition to the inspection by the government supervisor's / regulators, Does the institution have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?		
41	what is the frequency of AML audit carried out by internal		

✓ 8

g

KYC, AML/CFT Procedural Guidelines-2018

	auditors?	
42	Does your Regulatory Supervisory Authority conduct regulatory examination on a regular basis, to assess you AML/CFT?	
43	State the sanction lists that the entity is currently using. (OFAC/UN SANCTION/US SANCTION/HMT/SDN/ETC or Others.	

SANCTIONS AND PEP SCREENING

44	what is the current PEP and sanctions screening process? If manual mention the procedures.	Automated	Manual	Others
----	--	-----------	--------	--------

KNOW YOUR CUSTOMER, DUE DILIGENCE AND ENHANCED DUE DILIGENCE

45	Does the entity offer services to individuals using fictitious names or who refuse to disclose their identity or conduct financial transactions on behalf of other persons?	
46	Does the entity allows to conduct the transactions on behalf of Other persons?	
47	Does the entity provide services to shell entities?	
48	Does the entity deals with offshore entities?	
49	does the entity have procedures for the identification of the direct/ indirect customers on whose behalf it maintains or operated accounts or conducts transactions?	
50	Does the entity assess its customers' AML policies or practices?	




KYC, AML/CFT Procedural Guidelines-2018

51	Does the entity have procedures to review and, where appropriate, update customer information relating to high risk client information?	
52	What is the frequency of CDD and ECDD conducted?	

TRANSACTION MONITORING AND REPORTING

53	Does the entity file Suspicious Activity/Transactions reports as required by the Law of land?	
54	Does the entity file Threshold Transaction Reporting as required by law of land?	
55	Where cash transaction reporting is mandatory, does the institution have procedures to identify transactions structured to avoid such obligations?	
56	does the entity facilitate any TTs/International Payments on behalf of non-customer?	
57	Does the entity apply KYC Procedures on wire transfer. If limit applies, mention it.	
58	Does the entity allow any external party to access directly any correspondent account that the entity maintain with another FI for the purpose of facilitating payments (i.e. nested/payable through accounts)?	

AML TRAINING

59	Does the entity provide AML training to relevant employees? If yes to above, what is the frequency of AML training for staff?	
60	Does the entity communicate new AML related laws or changes to existing AML related policies or practices to relevant employees	
61	Does the entity employ third parties to AML related functions? Who is ultimately responsible for the functions?	




KYC, AML/CFT Procedural Guidelines-2018

DOCUMENTS TO BE ENCLOSED IN SUPPORT

A. Certified copy of certificate of incorporation	
B. Certified copy of License	
C. List of Branches/subsidiaries under which the Branch/subsidiaries Operate	
D. certified copy of documents Evidencing Name Change	
E. List of Shareholders holding 10 % and Above.	
F. AML/CFT Policy of the entity	

CONFIRMATION AND AUTHORIZATION

I confirm that in completing and signing this form, I am authorized to provide the above responses on behalf of the Entity	
Name of Compliance Officer	
Designation	
Address	
Telephone	
E-mail	
Signature	
Date:	

Annexure-10: Database of PEPs, Influential Persons and High Ranking Officials

S. No.	Name of the Person/ Entity	Affiliated Institutions/ Party	Address

(Signature)

Jo

Annexure-11: Recording of correspondence from Various Authorities

S. N o	Letter reference Number	Lett er Date	Letter received from	Letter received Via	Lett er type	Name of the Person / Company	Addres s of the Person/ Company	P A N NO	Proprie tor Name	Proprie tor Address	Fath ers Name	Gran d Fath ers Name	Cit ize ns hip No	Acc oun t Fou nd or Not	If found menti on Acco unt Num ber	Lette r Repli ed Date




Annexure-12

Details of Board of Directors/Executive Committee
Name Of Organization:-

S.No	Name	Position	Occupation	Grand Fathers Name	Fathers Name	Mothers Name	Spouse Name (for Married)	Current Address (Ward No, Municipality, District)	Mobile No	Citizenship No	Email Address
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											
25											

Company Stamp

Certified By
Designation
Date:-