EXTRACT OF AML/CFT/KYC POLICY AND PROCEDURE- 2014

5th Revision, June 2021

(Approved by BOD Meeting dated 29th June 2021)

2nd Revision November 2017

3rd Revision December 2018

4th Revision January 2020

HBL हिमालयन बैंक लिमिटेड Himalayan Bank Ltd.

Background

To ensure that funds generated through illegal activities are not channeled through the financial system of a country irrespective of its origin, the Financial Action Task Force (FATF) established by countries of Group of Seven (G7) has come up with strong recommendations against criminal activities related to money laundering and terrorist financing. Since Nepal is a member of the Asia Pacific Group on Anti-Money Laundering (a FATF-style regional body), it is the duty of every financial institution of the country to check and control money laundering-related activities. As these institutions' activities extend beyond the political boundaries of the country, it would be pertinent to devise/implement processes on anti-money laundering that are appropriate by the international standard.

Nepal, in line with directions from FATF, has promulgated the Asset (Money) Laundering Prevention Act, 2008 with a view to addressing issues relating to money laundering. The Act mainly directs and forbids banks and financial Institutions not to collect from customers deposits (funds) that come from illegal sources.

The Act clearly defines that banks and financial institutions should not be involved even in helping its customers to conceal, transform, transfer or hide the sources of funds or misrepresent them. They should immediately inform details of such funds/transactions to the Financial Information Unit (FIU) at Nepal Rastra Bank (NRB) (the Central Bank of Nepal), a focus center that has been established under the Act and is the main concerned authority for controlling/monitoring deflection of currency or money laundering in Nepal.

Himalayan Bank Limited is committed to developing and implementing appropriate policies and procedures to control AML and CFT and follow KYC policy guideline and update them on a timely basis in line with the changing environment, both on domestic and international fronts.

This policy document has been prepared in line with the guideline provided by the FIU and the Central Bank (Nepal Rastra Bank) under the purview of “the Asset (Money) Laundering Prevention (Second Amendment) Act, 2014” (ALPA) promulgated by Parliament, Anti-Money Laundering Prevention Rules 2073 (October 2016) and Directives issued by the FIU and the NRB from time to time.

However if there is any change in the regulations, act or Directives of the Central Bank and the government regarding AML/CFT/KYC issues after implementation of this policy, it will supersede this policy.

Key points in policy:

The policy shall include guidelines for ample controls, processing and procedures to be followed to have proper insight into entities and individuals with whom the Bank is dealing so that they are properly known, and their transactions can be monitored by the Bank.

The policy shall incorporate the following broad key elements:

1. Policy and procedure : Detail Policy and Procedure is elaborated in our main Policy. Brief of Policy is given below:

2. Money Laundering/Combating Financing Terrorism

Money laundering is the process where the source of illegally obtained funds is channeled through a series of transfers and deals that can eventually obscure its original source and present it as legitimate income or assets. The amount involved can be large at times. However, it can also be broken into small amounts and collected ransoms in order to bury its originating source or use in criminal activities.

It is not necessary that money earned through illegal sources and converted into clean ones is the only form of the process that falls under the money laundering activity. Even legally earned money that changes hands for the purpose of financing illegal activities is considered illegal. Therefore, the process of funds being tied up during any stages of an illegal activity can be identified as money laundering. Furthermore, illegally earned money does not merely comprise funds earned from drug trafficking, prostitution, illegal arms dealing and terrorist activities but also includes money collected through corruption, tax evasion and other criminal activities where the owner cannot disclose its originating source.

1.1 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, money obtained illegally is brought into the financial system through financial institutions.

1.2 Placement

The physical disposal of cash proceeds derived from illegal activities could be done through:

i. Depositing a large amount of cash in numerous small amounts, a process called smurfing.
ii. Hoarding deposits in the name of others enjoying tax blanket/exemption.
iii. Setting up a cash business as a cover for banking large amounts of money.
iv. Investing in shares and other investment products.
v. Mingling illegal cash with deposits from legitimate business, e.g. car and antique dealers.
vi. Hoarding deposits in the name of persons instead of in the name of companies to avoid higher taxes.

1.3 Layering

Layering is the practice of separating 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. Examples are as follows:

i. A company passes money through its accounts under cover of bogus invoices merely to generate additional transactions.

ii. A customer raises a loan on the security of a deposit (from illegal business) from another bank to help break the connection with illegal funds.
iii. A customer incurs large credit card debts from an account.
iv. A customer buys in cash and en-cashes it against the bank trail.

1.4 Integration

If the layering process succeeds, 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 origin.

2. Customer Identification Procedures (CIP) (ALPA: 7A)

The CIP is a process of identifying the customer and verifying his/her identity by using reliable, independent supporting documents or data or information, including that available in the third-party-database. The designated staff must obtain sufficient information to establish the identity of each new customer along with the intended purpose of the relationship. Customer Identity can be accurately identified when carrying out the following acts:

i. establishing business relationship
ii. opening an account
iii. carrying out occasional transactions above the threshold
iv. carrying out fund transfer by electronic means
v. suspicion about the veracity or adequacy of previously obtained customer identification information
vi. suspicion about money laundering or terrorist financing
vii. performing transaction(s) any time in relation to the high risk and politically exposed persons

The CIP is carried out to satisfy the Bank and other competent authorities that the due diligence process has been carried out based on the risk profile of the customer and potential risk associated with it has been checked. Such a risk-based approach is considered necessary to avoid disproportionate cost to the institution and ease the burden on the customer. Besides the risk, the nature of information/documents required also depends on the risk category of the customer.

Branches and the concerned departments shall take the following measures when identifying and verifying the customer.

i. understanding and obtaining information and details clarifying the objectives, purpose and intended nature of business relationships and transactions.
ii. where the customer is a legal person or legal arrangement, understanding and verifying their ownership and control structure and obtaining such information.
iii. when a person is establishing business relationships or conducting transactions on behalf of another customer, obtaining identification

documents of such a person and the person working on behalf of him, including evidence verifying that the person is properly authorized to act.

3. Customer Acceptance Policy (CAP)

The Bank Customer Acceptance Policy (CAP) lays down the following explicit criteria for accepting customers:

i. An account shall be opened only in the name of a natural or legal person. The name should be exactly the same and consistent with the one appearing in the identification document. No account should be opened in anonymous or fictitious/blank name(s) or with a confidential account number (ALPA:6).
ii. Minimum information and documents must be obtained from the customer for account opening, purchase of a foreign draft, transfer of funds through any medium, accepting of funds through any medium or carrying out transactions for the reasons as mentioned in detail Policy as well as in Customer Service Manual of the Bank.
iii. No account shall be opened by an intermediary for a third person.
iv. No account shall be opened without face-to-face contact with the customer. (The account opened by a representative officer/market representative/ correspondent partner of the Bank shall be treated as the account opened by the staff itself)
v. An account opened with insufficient documents shall be marked as “post no debit” and no cheque book shall be issued against such an account.

4. Customer Due Diligence (CDD):

Customer Due Diligence (CDD) is a key part of the process wherein the Bank conducts voluntary investigation to justify the underlying transactions against necessary documents but not for any legal implication/purpose. CDD is the process of identifying (CIP) and evaluating the customer and assessing customer risk as part of KYC. This process helps the Bank to determine whether the customer is a low-risk, high-risk or medium-risk customer and make the CAP accordingly. Customer Acceptance and Customer Due Diligence (CDD) refers to the process of identifying the true identity of the customer dealing with the Bank, creating a profile of the same, profiling in line with risk parameter/exposure, etc.

5. Ongoing due diligence:

Ongoing monitoring is an essential element of the effective CDD process. Customer transactions shall be monitored automatically or manually, whichever is feasible for the Bank. Compliance officers can effectively control and reduce the risks only if they have an understanding of normal and reasonable activities of a customer so that they have the means to identify irregular patterns of transactions. However, the extent of monitoring depends on the risk sensitivity of the account. Compliance officers should pay special attention to all complex, unusually large-value and/or

unusual patterns of transactions that have no apparent economic or visible lawful purposes.

6. Enhanced Customer Due Diligence (ECDD):
Enhanced Customer Due Diligence is conducted for high-risk customers. It refers to the additional due diligence pertaining to the identity of the customer, source of income, nature and value of transactions and others as specified by the relevant directives.

7. Know Your Customer (KYC)

Know your customer (KYC) is the due diligence and regulation that the Bank must carry out to identify its customers and extract relevant information about financial transactions carried out with it. KYC policies are becoming increasingly important in the global arena to prevent theft, fraud, money laundering and terrorist financing.

One of the key aspects of KYC is to verify that a customer/prospective customer is not enlisted as a fraudster, terrorist or money launderer or is not regarded as high-risk or carries a negative report in the media/public records. It is necessary to quantify the risk factor associated with the client/customer and prepare a process to mitigate the risk associated with the Bank/ transactions.

8. Customer due diligence/KYC update time interval and beneficial owner update:

For High Risk: Annual
Medium Risk: 4 Years
Low Risk: 5 Years

9. Simplified KYC/Simplified Customer Due Diligence (SCDD)*:*

This can be conducted for customers who fall under the low-risk category having characteristics as specified by the NRB directives such as the total annual deposit or transactions remaining within the limit of NPR 100,000, financial institutions supervised by NRB, customers whose identity is publically available and controlled by the national system and others as specified by the regulator from time to time.

10. KYE – Know your Employee

In recent times, it has become necessary to know your employee well and conduct their due diligence process. This therefore brings into sharp focus the need for thoroughly checking employees' credentials and properly screening candidates to prevent undesirable candidates from being hired. Separate forms shall be developed and details about employees of the organization shall be collected by the Human Resource Department.

A good internal control system with a strong and robust ethical culture minimizes any damage. AML guidelines prescribed by the regulator must be implemented and followed rigorously.

The HBL Staff Service Rules with the Code of Conduct are vital documents for addressing HR issues of the organization.

11. Risk Categorization - High Risk /Low Risk/Medium Risk:
It includes those types of customers or countries identified as 'high risk' by international agencies in view of their exposures to activities related to money laundering, drugs, terrorism, propensity to or history of public corruption, organized crime, fraud, human rights abuses, non-existent or inadequate financial regulations and fictitious or non-recognized jurisdictions that issue fraudulent financial service licensing and international sanctions (including special measures, financial havens with banking secrecy, uncooperative tax havens, a weak regulatory framework for alternative remittance systems and offshore financial centres).

The list also includes alerts for pseudo-official or non-government jurisdictions or entities that issue camouflaged or spurious passports.

12. Compliance Officer(s)

Compliance officers/KYC officers are the designated staff of the Bank stationed at Head/Corporate Office and/or a branch to ensure day-to-day compliance with internal policies/procedures related to AML/KYC or CDD and/ or make ongoing evaluation of the efficacy of the policies and procedures. They should be the focal points for managing AML/KYC and CDD-related matters.

13. Beneficial Owner - Identification of a beneficial owner, keeping record of the beneficial owner with complete KYC details:
A beneficial owner is 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 or shareholder possessing 10% or more shares or voting rights. The system is required to detect such a beneficial owner as per the NRB Directives.

14. Sanction Programs:

The Bank has its own Swift Sanction Screening software to screen and put on hold the remittances received from banks and financial Institutions under OFAC and the other sanction list on a real-time basis. The concerned staff shall check the screening before releasing all the inward and outward payments.

While opening an account, it is the responsibility of the concerned staff to screen the transactions against the PEP/PIP/sanction screen mandatorily. Also before processing LC and loan proposals, the concerned RM shall screen the applicant and the beneficiary. In case of matching, the Central Operations and CICD shall be notified before taking appropriate action.

15. Domestic High-profile Person/ Domestic Politically Exposed Persons (PEP)

Domestic high-profile or politically exposed persons include any person who is or has been in the post of special class or equal thereto or above of the Government of Nepal, a judge of High Court and above, a senior politician, a central committee member of a national political party, a senior executive of any institution partially or fully owned by the state, the President, the Vice-President, a ministers or a parliamentarian. Likewise, in Province Level, Chief Ministers, ministers, speakers and deputy speakers are also PEP. Mayors of municipalities, and chairman of Rural Municipalities are also PEP. It also includes other groups of persons as designated by the Government of Nepal on the recommendation of National Coordination Committee and family members of PEP (definition of family members is mentioned in detail in main Policy

People in the influential position (PIP) include the Chairman, CEO, and Board members of a public entities.

16. High net worth Individuals: The criteria for determining such individuals shall be fixed by the Management from time to time.

17. Foreign High-profile persons/foreign politically exposed persons

Politically exposed persons include the Head of State or Government, a senior politician, a central member of a national political party, a senior government official, a judicial or military official or senior executives of state-owned corporations of a foreign country.

18. Risk-based Approach (RBA)
It is the approach of the management which focuses on identifying and addressing potential risks of money laundering and terrorism financing. The core of this approach is to match risks and controls by understanding the ML/TF risks to which the Bank is exposed and apply AML/CFT measures in a manner and to an extent that would ensure mitigation of these risks. There is no universally accepted methodology that prescribes the nature and extent of a risk-based approach. It provides every bank with flexibility to manage its ML/FT risks in its own way.

19. Suspicious Transaction:

A transaction, including an attempted transaction, whether or not made in cash, which a person conducts purportedly in good faith, may gives rise to reasonable grounds of being a suspicious transaction that may involve proceeds of an offence specified in the law and regulations regardless of the value involved.

Such a transaction has the following features:

Seems to conceal or disguise the nature or origin of funds derived from illegal

Activities.

Seems to have no economic rationale or bona fide purpose.

Seems to be unusual or unjustified and complex in nature.

Seems to be deviated from profile, character and financial status.

Seems to be made for the purpose of evading the legal and regulatory reporting requirements.

Seems to be conducted to support the activities relating to terrorism.

20. Suspicious Transaction Report:

A report shall be made by the Bank and submitted to the FIU on any suspicious transactions or any attempts under the provisions of "Pariched 3, 7dha- Asset (Money) Laundering Prevention Act 2064" and Point No. 14 of NRB Directive No. 19.

21. Wire Transfer:
Any transaction carried out on behalf of an originator (both natural person and legal entity) through the Bank by electronic means with a view to making an amount of money available to a beneficiary person at another FI. The originator and the beneficiary may be the same person.

22. FATCA Reporting:
The Bank shall comply with FATCA as per the requirements of the US Law and NRB Guidelines.

23. Confidentiality:

Anyone who violates the confidentiality pursuant to subsection (2) of section 10B or section 26 shall be punished with imprisonment ranging from one month to three months or fined up to one hundred thousand rupees, or both (for tipping off).

24. Complete Record-keeping (ALPA:7R)

All the documents and records related to ML and TF shall be maintained accurately and securely for a minimum of five years from the termination of business relationships or from the date of transactions in case of occasional transactions. The following documents or records or information shall be kept safely as per the following arrangements:

1. All documents and other information related to the identification and verification of customers and beneficial owners.

2. All documents, records and conclusions of the analysis of a customer or a beneficial owner and transactions, including customer identification documents, shall be placed in customer files. It is the responsibility of the Customer Service Department of a branch to ensure this.

3. Customer identification and transaction documents shall be retained for at least 5 years after closure of the accounts/transactions.

4. Documents and details of accounts and business relations.

5. All documents and records relating to domestic and foreign transactions.

6. Record and documents on attempted transactions.

7. Records of all suspicious reports and reports submitted to the FIU and/or other concerned authority shall be safely maintained. Where a suspicious report does not result in a report to be submitted to the FIU or other authorities, the reason for such a decision shall be recorded.

8. Other documents and records as prescribed by the regulator.

10. Notwithstanding anything written in subsection (1), the reporting entity shall keep some prescribed documents and records for more than five years securely as prescribed.

11. The reporting entity shall keep and maintain documents and records pursuant to subsection (1) and in such a way that it shall be sufficient to reconstruct such information for the use of legal action as evidence.

12 Documents and records to be maintained pursuant to this section should be kept in such a way that it could be made readily available to competent authorities upon demand.

13 The reporting entity shall keep the reports of suspicious transactions for five years.

14. The other provision on records and reports of transactions of reporting entities shall be as prescribed.

15. Records of all training related to ML and TF provided for staff shall be maintained. Such records also include the nature and names of staff that have attended the training. The staff who undergo the training shall sign the records with dates. The initiative shall be taken in keeping the records digitally as required by the Central Bank.

25. Awareness and Training of Staff on AML/CFT

All staff should be aware of the statutory and regulatory obligations. Therefore, the designated compliance officer at Head Office or the person assigned by the compliance officer shall be responsible for conducting employee training programs in coordination with the Human Resources Department on an ongoing basis so that all the concerned staff are adequately trained on AML/KYC and CDD policies/procedures. The training requirements may be different for the front-line staff, compliance staff and staff dealing with new customers. However, initial training should be provided to all staff on money laundering and terrorist financing activities and means to control/counter them. The staff shall be regularly updated on any change of responsibilities.

Training shall be conducted for all staff, stationed in and outside the Valley, time and again in coordination with the Human Resources Department and Central Operations Department. Training on AML/CFT/KYC issues should be mandatory for all front-line and operations staff. Such training should also include other employees of the Bank.

The training should be focused on AML/CFT risks, the latest regulatory guidelines, corporate governance, KYC, money laundering, etc. as per the latest directives from the Central Bank.

Effective discussions with participants should be held and their queries should be addressed. Half-hour training assessment with respect to AML/CFT to map out the understanding of participants should also be made.

The Human Resources Department should conduct a written examination after the KYC/AM/CFT training so as to gauge the participants' understanding of the subject.

The Bank's concerned staff should be sent for training on AML/CFT at national as well as international levels.

CICD, in coordination with the Human Resources Department and Central Operations Department, should arrange for knowledge-sharing programs on the latest developments in the subject.

Shareholders holding shares above 2%, Board members and senior executives should also participate in the AML/training every year. Remittance agents and sub-agents should attend the training on AML/CFT conducted by CICD on a yearly basis. Soon after recruitment, induction training on operations as well as AML/CFT issues should be conducted compulsorily.

26. Correspondent Banking Relationship (ALPA:7M):
Prior to establishing relations with correspondent banks, the Bank shall gather sufficient information about their correspondent banks or financial Institutions to fully understand the nature of their business. The Bank shall undertake such CDD on establishment of every correspondent banking relationship by benchmarking information received from third parties and/or information available in public domains. Factors to be considered should include information on its management, major business activities, location of business, money laundering prevention and detecting efforts, purpose of the account and proper identification and CDD of third parties using the correspondent banking network. Annual CDD is mandatory for Vostro and Nostro accounts with negative publicity; and remittance agents, super agents and sub-agents. The questionnaire as mentioned in main policy should be obtained from correspondent partners to gather sufficient information.

The correspondent bank or financial institution should not be a shell company or located in non-cooperating countries and territories as categorized from time to time by FATF or other regional types of FATF such as APGA. Approval of the senior management should be obtained before establishing a new correspondent relationship.

27. Internal Control: the Board of Directors shall formulate and develop necessary policy procedure or controlling systems on the basis of "the Asset (Money) Laundering Prevention (Second Amendment) Act, 2014" (ALPA) promulgated by Parliament, Anti Money Laundering Prevention Rules 2073 (October 2016) and AML Directives issued by the Central Bank.

28. Threshold Transaction Report (TTR):
The Bank should report following limits of transactions to the FIU within fifteen (15) days of the transactions as per the format mentioned in main policy.

i. Single or multiple cash transactions by a customer in a day to the tune of rupees one million or above or up to the limit set by the concerned authority from time to time.

ii. Single or multiple remittance transactions by a customer in a day to the tune of rupees one million or above or up to the limit set by the concerned authority from time to time.

iii. Single or multiple exchange transactions by a customer in a day to the tune of rupees of five hundred thousand or above or up to the limit set by the concerned authority from time to time.

For any cash transaction above the threshold limit, the declaration of the source of funds should be disclosed by the customer in the deposit slip and the same should be updated in the core banking system (CBS).

The Bank shall have a dedicated department- the Compliance and Internal Control Department (CICD) to monitor the threshold and report it to the Central Authority as prescribed in the Act. Threshold transaction data should be downloaded by incorporating the entire database in the core banking software (CBS). Any transaction which matches and/or exceeds the prescribed threshold parameter shall be reported to the FIU. Prior to reporting, the CICD shall undertake proper investigation into the account database, transactions details, etc. and prepare a profile of the customer with a copy of the report forwarded to the management. The Bank shall ensure that the concerned department is well equipped and has adequate manpower to meet the growing challenge on the AML/CFT front so that monitoring and reporting of suspicious transactions can be made in a timely manner.

29. Roles and Responsibility of Board of Directors, Senior Management and Individual Employees: Roles and responsibilities of respective stake holders is mentioned in main AML/CFT/KYC Policy and Procedure 2021.

30. Punishment Clause: Various Punishment Clause for noncompliance related to AML/CFT is detailed in main Policy.