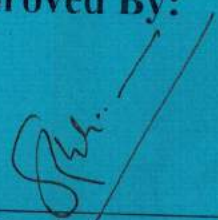
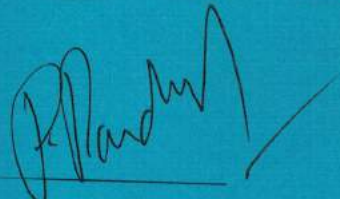




## I PAY REMIT AML & CFT POLICY

This AML & CFT Policy has been conceptualized, formulated and approved by Board of Directors of I PAY REMIT PVT. LTD. This policy guides all the Compliance behaviors, rules, regulations and implications to be followed and monitored at all times.

**Approved By:**

  
\_\_\_\_\_  
Chairman  
\_\_\_\_\_  
Director  
\_\_\_\_\_  
Executive Director  
\_\_\_\_\_  
Director  
\_\_\_\_\_  
Company Secretary

## I PAY REMIT AML & CFT POLICY

This AML & CFT Policy has been conceptualized, formulated and approved by Board of Directors of I PAY REMIT PVT. LTD. This policy guides all the Compliance behaviors, rules, regulations and implications to be followed and monitored at all times.

Approved By:

Chairman

Director

Executive Director

Director

Company Secretary



# TABLE OF CONTENTS

## CHAPTER I: INTRODUCTION

1.1 Overview of the Policy .....	7
1.2 Short Title of Policy .....	7
1.3 Definitions .....	7
1.4 Objectives .....	10
1.5. Purpose .....	10
1.6. Scope .....	11

## CHAPTER II: GOVERNANCE & THEIR RESPONSIBILITY FOR AML/CFT

2.1 Governance for AML/CFT .....	13
2.1. Roles and Responsibilities of I Pay Remit .....	14
2.1.1. Board of Directors .....	14
2.1.2. Risk Management Committee & Its Member .....	14
2.1.3. Executive Director .....	14
2.1.4. Money Laundering Preventive Officer (MLPO) .....	15
2.1.5. AML/CFT officer .....	16
2.1.6 Agents .....	16

## CHAPTER III: KYC AND MONITORING CUSTOMER

3.1 Know Your Customer/ Agent .....	18
3.1.1 Types of Customer .....	18
3.2. Purpose of KYC .....	19
3.3 Requirements of KYC .....	19
3.3.1 For Agents .....	19
3.3.2 For Customers .....	20
3.4. Mechanism Deployed for KYC .....	20
3.5 Nature of Transactions and Documents Verification Requirement .....	20

## CHAPTER IV: SUSPICIOUS AND THRESHOLD TRANSACTIONS

4.1 Suspicious Transaction .....	23
----------------------------------	----

4.1.1 Transactions of Suspicious in Nature .....	23
4.2. Threshold Transactions .....	23
4.2.1 Specific Criteria of Threshold Transactions.....	24
4.3. Indicators of Suspicious and Threshold Transaction .....	24
4.3.1 General Indicators.....	24
4.3.2 Specific Indicators .....	25
4.4. Elements of Suspicious and Threshold Transactions .....	25
4.5. Detection of Suspicious and Large Value Transactions.....	25
4.6. Terrorist Financing .....	26

## **CHAPTER V: MONITORING AND REPORTING SYSTEM**

5.1 Remittance Transaction Monitoring.....	27
5.1.1 Agent Transaction Monitoring .....	27
5.1.2 Remittance Review and Revision of Risk Level .....	28
5.2. Reporting Related to AML/CFT .....	28
5.3 Content of Reporting .....	29
5.4. Retention of Records .....	29
5.5. Policy Compliance .....	30
5.5.1. Employee and Agent Training Program .....	30
5.5.2 Amendment to the policy .....	30
5.5.3 Compliance Measurement.....	31
5.5.4 Exceptions .....	31
5.5.5 Non-Compliance.....	31
5.5.6 Repeal and Saving .....	31
5.6 Reporting through goAML Software .....	31

## **CHAPTER VI: BARRIERS FOR TRANSACTIONS**

6.1 Barriers for Transactions .....	32
-------------------------------------	----

## **CHAPTER VII: MISCELLANEOUS**

7.1 Correspondent and Shell Companies .....	33
7.1.1 Correspondent Companies .....	33
7.1.2 Shell Company .....	33

7.3.Miscellaneous Grounds for Suspicion..... 33



## LIST OF ABBREVIATION

ALPA - Assets Money Laundering Prevention Act

AML - Anti-Money Laundering

AOA - Articles of Association

BOD – Board of Directors

CDD- Customer Due Diligence

CFT - Counter Financing of Terrorism

CIAA - Commission for the Investigation of Abuse of Authority

DC - Digital Certificate

DNFBP - Designated Non-Financial Businesses and Professions

ED – Executive Director

FATF - Financial Action Task Force

FCC - Financial credibility certificate letter

FIU – Financial Information Unit

ID - Identity Document

KYA – Know Your Agent

KYC – Know Your Customer

ML - Money Laundering

MLPO - Money Laundering Preventive Officer

MOA - Memorandum of Association

NRB – Nepal Rastra Bank

OFAC- The Office of Foreign Assets Control

OIC – Officer In Charge

PEP - Politically Exposed Person

RM – Regional Manager

RMC – Risk Management Committee

STR – Suspicious Transaction Report

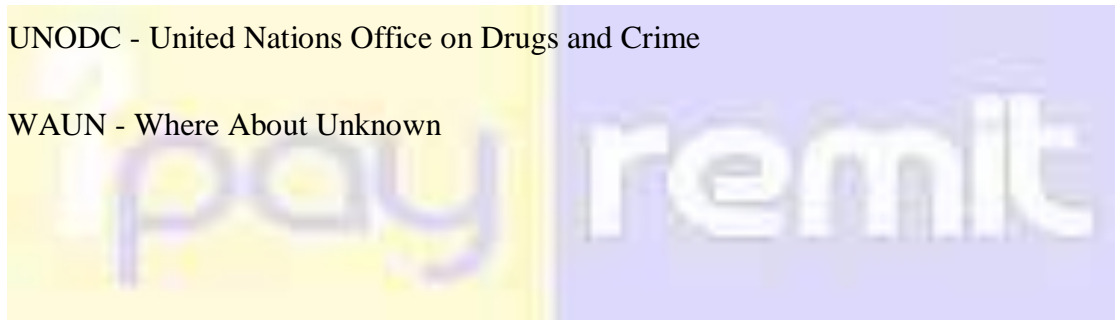
TF – Terrorism Financing

TTR - Threshold Transaction Reports

UN – United Nation

UNODC - United Nations Office on Drugs and Crime

WAUN - Where About Unknown



# CHAPTER I

## INTRODUCTION

### 1.1 Overview of the Policy

The AML/CFT POLICY have been designed to guide the action and govern the right of the Company. The policy has been designed and approved by Management of I Pay Remit Pvt. Ltd. In lines with the Company's Articles of Association (AOA) under Section 5 (4) and as per NRB guidelines, I Pay Remit reserve the right to add, change, revoke, suspend or terminate any or all of these policy either fully or in Part at any time, with or without Notice. If any such happens employees will informed of all such actions.

### 1.2 Short Title of Policy

This policy is called as "AML/CFT POLICY- I PAY REMIT PVT. LTD."

This policy comes into force from 2019 AD. and has been updated to Version 1.2; implementing from July, 2021 AD.

**1.3 DEFINITIONS:** Under the subject or the context otherwise requires in this policy.

#### a) Money Laundering (ML)

Money laundering refers to criminal activities, such as drug trafficking, smuggling, human trafficking, corruption and others, tend to generate large amount of profits for the individuals or groups carrying out the criminal act.

#### b) Terrorism Financing (TF)

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



### **c) Know Your Customer (KYC)**

KYC is the process of identifying the customer and verifying the identity by using reliable and independent document and information.

### **d) Customer**

Customer is any person or entity engaged in a financial transaction or activity with the company or someone on whose behalf the financial transaction or activity is being performed.

### **e) Financial Information Unit (FIU)**

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

### **f) Beneficial Owner**

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

### **g) Shell Company/Entity**

As per the Asset (Money) Laundering and Prevention Act 2008, Shell Companies are the financial institutions or a group of financial institutions that have no physical presence in the country of origin or establishment and/or do not fall under any scope of effective regulation and supervision.

### **h) Threshold Transaction Report (TTR)**

A Threshold Transaction Report (TTR) is a report that financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) are required to file to FIU-Nepal for deposit, withdrawal, exchange of currency, or other payment or

transfer; if it exceeds prescribed threshold limit. This guideline have been made and issued in exercise of power conferred by Assets Money Laundering Prevention Act (ALPA), 2008.

**i) Suspicious Transaction Report (STR)**

Suspicious Transactions Report are disclosure of financial transactions in which there are reasonable grounds to suspect that, the funds involved are related to the proceeds of criminal activity. What is reasonable depends on the particular circumstances, industry, normal business practices within the industry.

**j) goAML Software**

FIU-Nepal has now installed goAML software developed by United Nations Office on Drugs and Crime (UNODC). It will help for online receipt of reports and analyze such reports in an automated form.

**k) Legal Person**

Legal person refers to customer or agents or domestic as well as international business partners of I PAY REMIT PVT. LTD. considered as having many of the right and responsibilities of a natural person and especially the capacity to sue and be sued.

**l) Currency**

Currency for I PAY REMIT PVT. LTD. refers to both the convertible foreign currency and domestic currency.

**m) Money Laundering Preventive Officer (MLPO)**

Head- Compliance of the Remittance shall be the MLPO who would have the necessary freedom to act on his own authority and shall report to Executive Director. Name, Designation, Address, Qualification, contact number, e-mail address of the MLPO shall be informed to FIU for correspondence.

**n) Transactions**

Transactions for I PAY REMIT PVT. LTD. are domestic and international money transfer or account deposit transactions.

## **1.4 OBJECTIVES**

1. Comply with Anti-Money Laundering Act, 2064 amendment on 2070, legislation in the countries we operate in
2. Strive to fulfill international standards as detailed in the recommendations of the Financial Action Task Force (FATF)
3. Work in conjunction with the Nepalese Government and the governments of the countries we operate in, and support their objectives in relation to the prevention, detection and control of ML/TF
4. Maintain and comply with an AML/CFT policy, as required by Financial Information Units (FIU) under Nepal Rastra Bank (NRB)
5. Meeting its international regulatory obligations in the identification, treatment and management of ML/TF risk
6. Protecting the group from reputational risk and breaches of regulatory
7. Safeguarding the group, its customers and employees from becoming a victim of, or unintentional accomplice to, ML/TF activities

The company is intent on satisfying its local regulatory and international obligations in a sustainable manner.

## **1.5. Purpose**

This I PAY REMIT AML policy is based on the requirement of the section 7(TA) of Anti- Money Laundering Act 2064 (2nd amendment on 2070). Also this policy incorporates NRB directives, circular, agreed international rules and regulations and best practices, which directs I PAY REMIT Remittance activities to proactively comply with AML prudent practices among its stakeholders.

This policy's purpose is to establish governing standards to insulate the company from being used as a component of financial system to launder money.

In the light of above, the purposes of the policy are:

- To enable the company to conduct clean, money transfer business, conforming to standards set by the industry; laws and regulations of the country/governing authorities.
- To follow, the internationally accepted standards used for KYC compliance, as far as practical.
- To report and take suitable actions, upon detecting the suspicious activity involving shades of money laundering as directed by Nepal Rastra Bank or any other laws formulated from time to time by Government of Nepal.
- To make the employees and customers aware about the seriousness of the impact of ML activities.
- To set-up administration processes with the Agents to implement the set AML standards.
- To comply with applicable laws in Nepal with reference to ML and adhere to the standards accepted internationally by the financial world on the subject, as far as practical.
- To provide the knowledge to identify AML/CFT transactions.
- To make I Pay Remit staff aware of the AML/CFT policies and practices.
- To avoid the Processing of anonymous, UN sanctions list and fictitious Remittance.
- To provide the knowledge to staff and agent to verify the identity of prospective customers before they collect their Remitted Amount.

## **1.6. Scope**

The four basic tenets of AML have been covered in this policy. They are:

1. Know Your Customer/ Know your Agents (KYC/KYA)
2. Risk Assessment of Transaction.
3. Transaction Review
4. Suspicious and large Value Transaction Monitoring and Reporting

This policy also intends to increase the awareness of ML activities amongst the staff, agents, customers and general public and its ill effects and also effectively counter/guard against ML at all times.

There is a specific law “Anti- Money Laundering Act 2064, 2nd amendment on 2070” prevailing in the country on this. Nepal Rastra Bank has also formulated guidelines on KYC. Considering the sensitiveness of the matter on global arena the Company has developed this Policy in order to be proactive in dealing with issues related with ML within the preview of the local law and guidelines of Nepal Rastra Bank.

Compliance and willing adoption of this policy will be the primary goal while implementing it. All I PAY REMIT employees and affiliates must comply with this policy.

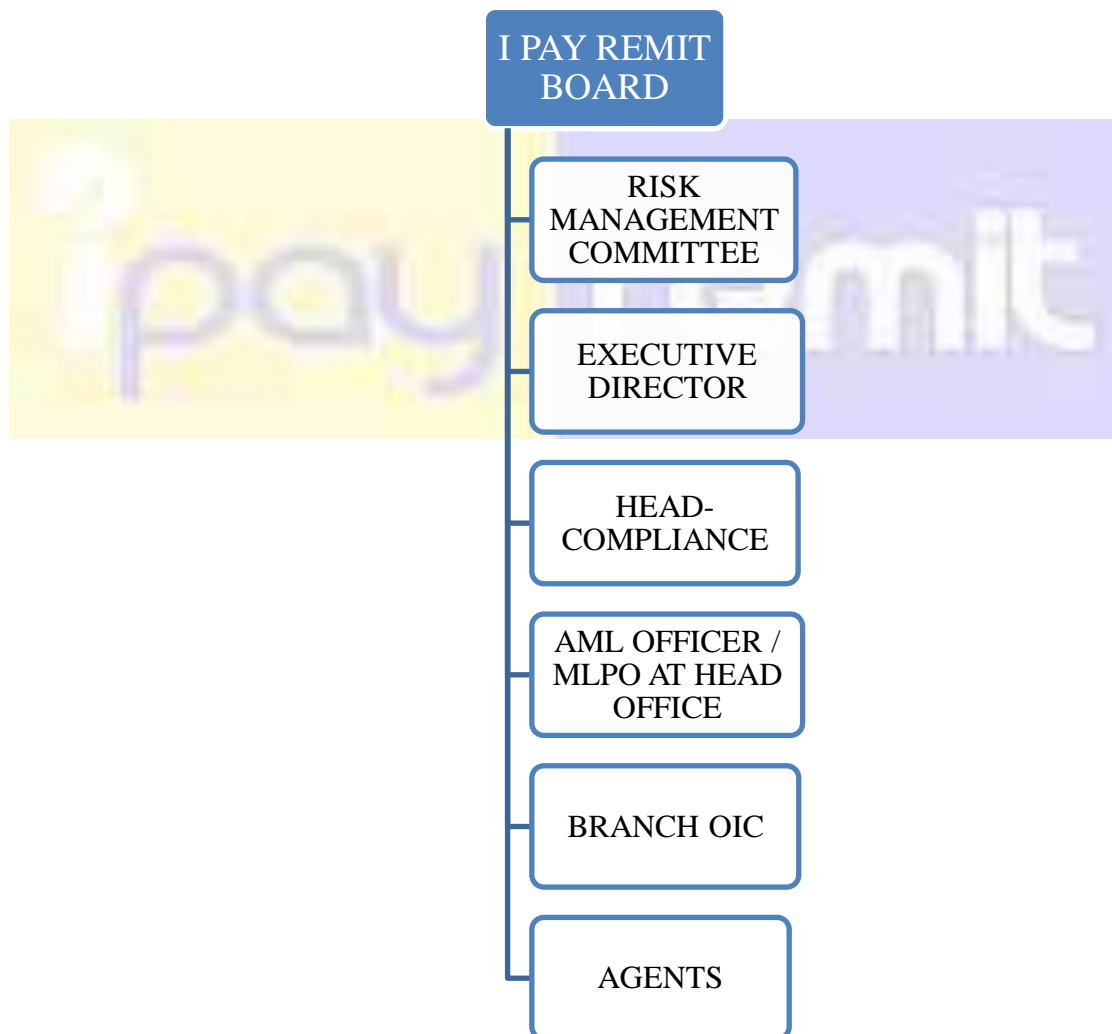


## CHAPTER II

### GOVERNANCE & THEIR RESPONSIBILITY FOR AML/CFT

#### 2.1 Governance for AML/CFT

Governance structure assigns responsibilities for the design of the company AML/CFT implementation and monitoring structure and overall accountability for results. To align with over business requirements, it incorporates guidance from global standards, NRB Circulars and Directives and elements consistent with evolving best practices. A key element of our compliance governance structure is at below:



## **2.1. Roles and Responsibilities of I Pay Remit**

The section below details the various roles and responsibilities of governance structure of I Pay Remit for AML/CFT compliance.

### **2.1.1. Board of Directors**

- Approving, enforcing internal AML/CFT policy;
- Establishing and approving the organizational structure, roles and responsibilities in AML/CFT of individual/department/unit;
- Oversight on the risk management on AML/CFT.

### **2.1.2. Risk Management Committee & Its Member**

- RMC member constitutes of Executive Director & All Departments Head of I Pay Remit.
- RMC will Review and support AML/CFT policy for the purpose of approval from Board of Directors.
- RMC will Periodically reviewing and updating AML/CFT policy
- RMC will be Monitoring AML/CFT related activities to implement AML/CFT policy.

### **2.1.3. Executive Director**

Ensuring that the policies and procedures for AML/CFT Program are in line with changes and developments in products, services and information technology of the Company as well as in line with development in modus for money laundering or terrorist financing.

- Ensuring that the implementation of AML/CFT Program is based on established policies and procedures.
- Ensuring that all employees, particularly employees of related work units and new employee have participated in ongoing training related to AML & CFT Program.
- Supervise the compliance department work in implementing AML & CFT Policy and procedure.
- Review and approve all AML/CFT procedures.

- Monitoring whether the TTR and STR has been updating within the certain time period to FIU
- Report quarterly to BOD on the compliance of AML/CFT Act/Rules/Directives issued by Nepal Rastra Bank. Such report shall be submitted to FIU on half yearly basis.

#### **2.1.4. Money Laundering Preventive Officer (MLPO)**

Head- Compliance of the Remittance shall be the MLPO who would have the necessary freedom to act on his own authority and shall report to Executive Director. Name, Designation, Address, Qualification, contact number, e-mail address of the MLPO shall be informed to FIU for correspondence.

The Roles and responsibilities of the MLPO shall be as follows:

- Submit Suspicious Transaction report to FIU within 3 days.
- Individual suspected while doing transaction.
- Suspected to be involved in illegal organization related to ML/TF.
- Suspected to have such intentions of performing illegal transaction.
- Communicate Money Laundering Prevention requirements to all staff periodically.
- To ensure laid down procedures on AML/ Customer Due Diligence (CDD) are followed in all units.
- To perform activities as required under Anti Money Laundering Act, rules, directive issued by concerned authority.
- To develop and implement effective AML/CDD procedures for internal use.
- Ensure good coordination between operations and top management.
- To ensure timely reporting and maintenance of records of transactions exceeding threshold limit set by the regulators.
- To carry out trainings to all staff on AML/CDD.
- Report quarterly to BOD through Executive Director on the compliance of AML/CFT Act/Rules/Directives issued by Nepal Rastra Bank. Such report shall be submitted to FIU on half yearly basis.
- MLPO has authority to look after the documents and inquiry to all the department of the organization regarding ML/TF.



- Any changes in the policy by FIU/Governemnt of Nepal, MLPO should adapt and follow it.

### **2.1.5. AML/CFT officer**

Designated officer at Compliance Department and Operation in charge of the branches shall act as AML/CFT (Anti Money Laundering/ Counter Financing of Terrorism) Officer.

The major responsibilities of AML/CFT Officers will be as follows:

- To ensure compliance to AML Act 2008 along with internal AML Policy and AML/CDD procedures.
- To authenticate Know Your Customer / Know your Agent (KYC/KYA) as required under AML/KYC procedures.
- To maintain record of Know Your Customer / agent information as prescribed under AML/CDD procedure.
- To maintain record of transaction exceeding threshold limit and to file Transaction Threshold Report on fortnightly basis to Compliance Department.
- To ensure all staff of the branch and agents have carried out in-house training on AML/CFT at least once every year.
- To file suspicious transactions reports to Compliance Department of the transactions which do not match with general financial condition of the customer.
- To keep customers information confidential at all time.
- Whilst managing overall AML activities is the responsibility of Head Compliance, AML/CFT officers of the branches will liaise with AML/CFT officers at Head office for any AML/CFT related issues of their respective branches on an ongoing basis.

### **2.1.6 Agents**

The agents should be responsible for all the conditions as mentioned during the agreement, and need to follow the acts regulated by NRB as well as AML/CFT policy of I Pay Remit Pvt. Ltd.. Furthermore, the responsibilities of agents will be as follows:

- To collect the valid Government Identity Document (ID) of the customer during payment receivable.
- To retain the proof of payments including customer's valid ID and voucher slip/withdrawal slip for 5 years.
- To update and report Head Office regarding the suspicious as well as threshold transactions.
- To provide the required documents to Head office in case of inspection and investigation by compliance department.
- To record customer's information appropriately and keep it confidential all the time.
- To ensure all the staffs have proper training and knowledge about compliance rules and policies.



## CHAPTER III

### KYC AND MONITORING CUSTOMER

#### 3.1 Know Your Customer/ Agent

Know Your Customer/Agent (KYC/KYA) is the process of a business verifying the identity of its agents and clients. The term is used to refer to the Remittance regulation which governs these activities. Remittance industry is increasingly demanding that customers provide detailed anti-corruption due diligence information, to verify their probity and integrity. Know your customer policies are becoming much more important globally to prevent identity theft, financial fraud, money laundering and terrorist financing. I PAY REMIT shall not engage in business relationship for which customer identification and KYC is not performed.

##### 3.1.1 Types of Customer

###### a) Domestic Politically Exposed Persons (PEP)

The President, Vice-President, Minister, parliamentarians, officials of the constitutional bodies, officials remained in the special class or equal to special class or their senior of the Government of Nepal, judge of the Appellate Court and apex court and their senior, senior politician, central member of national political party or senior executives of any institution partially or fully owned by the Government. It shall also include other group of person as designated by the Government of Nepal upon the recommendation of National Coordination Committee. Further, the family member or close associate of the PEP are also considered as PEP.

###### b) Foreign Politically Exposed Persons (PEP)

Politically exposed person who is or has been the Heads of State or of government, senior politician, central member of national political party, senior government, judicial or military official, senior executives of state owned corporations of a foreign country. Further, the family member or close associate of the PEP are also considered as PEP.

### **c) General Customer**

General customer are those who have not being involved in Head of government, politics, national political party, judicial or military official, state owned corporations of country. Further, they are the general citizens of the nation.

### **3.2. Purpose of KYC**

- To establish procedures to verify the identification of individuals or corporate or other institutional account.
- To detect suspicious transaction.
- To establish process and procedures to monitor high value and suspicious transactions.
- Establish systems for conduction due diligence and reporting of such activities.

### **3.3 Requirements of KYC**

#### **3.3.1 For Agents**

- Application
- Updated Registration Certificate
- PAN Certificate
- Copy of citizenship certificate of the Board Members
- Latest Audit Report
- Article of incorporation with remittance objective or letter of recommendation for operating remittance
- Application and Minute to start remittance business with I Pay Remit
- Tax Clearance certificate
- Cash Deposit / Bank Guarantee
- Location Map
- Photo of the office location (Inside and whole of outside)
- Education qualification (Minimum 5 Grade and above certificate)
- Utility bills/Proof of Address (electricity/telephone/water supply)
- Financial credinility certificate letter (FCC)
- Net worth certificate

- Bank Account Proof (Not older than 6 months)
- Article of Association and Memorandum of Association (AOA & MOA)
- Compliance Training Certificates
- Shareholder Certificate

### 3.3.2 For Customers

- Any Valid ID issued by Government of Nepal
- Contact number

### 3.4. Mechanism Deployed for KYC

The company shall use various mechanisms for Customer Due Diligence/ Agent Due Diligence Know Your Customer/Agent. These activities shall be carried out at the time of receiving Remittance for all the types of transaction Paid through I PAY REMIT. I Pay Remit shall deploy all or the combination of any of the below mechanisms for KYC/CDD.

1. Customer/ Agent identification and Profiling
2. Risk Assessment
3. Documentary Evidence
4. Verification of Documents as per original
5. Identification of Beneficial Owner
6. Politically Exposed Person (PEP) verification
7. Restriction on Receiving Transaction.

### 3.5 Nature of Transactions and Documents Verification Requirement

Based on the nature of transaction whether the transaction seems to be suspicious or meeting the threshold limit, compliance department can avail for the documents verification for further processing of the transactions. The criteria along with the probable documents requirements are mentioned below:

**(A) If the transaction amount meets or exceeds Rs. 1 million in sender or receiver side in one day or within a week either in single or in series of transactions, following documents are required to present:**

**In Individual Case:**

- Source of Fund (Proof of Documents)

- Purpose of sending Fund (Inbuilt in Remittance Form)
- Sender's Valid ID (Proof of Documents)
- Relation of sender with the beneficiary (Inbuilt in Remittance Form)

**(B) If the nature of transaction is created as Individual to Company Account, following documents need to be presented:**

- Sender's Valid ID (Proof of Documents)
- Purpose of sending fund i.e. commission, charge or any other (Proof of Document: Invoice or bill is a must as a supporting document).
- Source of Sending fund (Proof of Documents: Income Proof Supporting Documents)  
[Mode of Payment will be only Bank Account Deposit]

**(C) If the transaction is generated as Company to Company or Individual Transactions:**

- Attested Company/Firm Registration Certificate.
- Attested ID details of Sending Proprietor, Partner, Company Director and Individual Beneficial Owner.
- Purpose of sending fund i.e. commission, charge or any other (Proof of Document: Invoice or bill as supporting documents).
- Source of Sending fund (Proof of Documents: Income Proof Supporting Documents)

**(D) In case of sender founds to be in The Office of Foreign Assets Control (OFAC) listing or PEP, the Sender's valid Government issued ID needs to be presented.**

**Note:**

- In case of OFAC, the transactions cannot be proceeded.
- In case of PEP, Sender's valid ID documents which is followed by declaration of Non-Bribery needs to be submitted.
- If unable to present the supporting documents for purpose or source of sending fund, the declaration is required.

- iv. If required the KYC and further other documents needs to be submitted only in case of the Threshold or Suspicious transactions.



## CHAPTER IV

### SUSPICIOUS AND THRESHOLD TRANSACTIONS

#### 4.1 Suspicious Transaction

This section of the document is intended to highlight about the suspicious transaction and large value transaction. The Company will refuse any transaction where based on explanation offered by the customer or other information, reasonable grounds exist to suspect that the funds may not be from a legitimate source or are to be used for an illegal activity such as terrorism, human trafficking, drug abuse, weapon supplies etc. The Company shall use reasonable judgment in determining the suspicious transaction.

The understanding of customers' identity vis-à-vis his stated norms of dealings, services, etc would also have a bearing on transactions before they are viewed as suspicious transactions hence cautious approach in the process is very essential. Under no circumstances, company will alert a customer about his transactions being considered suspicious or that reporting is underway. The company will make prompt report of suspicious transactions, or proposed transactions to FIU through MLPO.

##### 4.1.1 Transactions of Suspicious in Nature

For identification of suspicious transaction, the Company shall take the precautions which would be exercised by a person of normal prudence. Some of the indicators of suspicious transaction shall be:

- Involvement of frauds for illegal activity.
- Intending to hide or disguise assets derived from illegal activities.
- Intention to evade AML guidelines.
- Customer has no business or apparent lawful purpose and has no linkage with such business.

#### 4.2. Threshold Transactions

A Threshold Transaction Report (TTR) is a report that financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) are required to file to FIU-Nepal for deposit, withdrawal, exchange of currency, or other payment or



transfer; if it exceeds prescribed threshold limit. The TTR limit for various reporting entities is different as per their nature and scope. TTRs are very important to develop the data bank of customers/clients profile for future use in case such transactions happen to be connected with money laundering and terrorist financing offences. TTRs also help to form a link chart during the analysis of a STR and help the investigator/analyst to find the criminal elements involved in the transactions and convert the financial information into financial intelligence by adding value in it. TTR is very important for both operational and strategic analysis. So in order to make filing of TTRs expedient for the purpose of aiding the financial analysis by forming financial intelligence from available financial information by adding value in it and preventing money laundering and controlling terrorist financing, this guidelines have been made and issued in exercise of power conferred by ALPA, 2008.

#### **4.2.1 Specific Criteria of Threshold Transactions**

The specific criteria for TTR are as follows:

- i. Reporting entities are required to file TTRs to FIU-Nepal within fifteen days from the date of transaction.
- ii. If the cash deposit transaction exceeds Rs. 1 million in one transaction or in a series of transactions in one day in single account.
- iii. If the cash withdrawal transaction exceeds Rs. 1 million in one transaction or in a series of transactions in one day in single account.
- iv. If the total of cash debit or credit transaction mentioned in ii) and iii) exceeds Rs. 1 million individually i.e either deposit total or withdrawal total.

#### **4.3. Indicators of Suspicious and Threshold Transaction**

##### **4.3.1 General Indicators**

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

### 4.3.2 Specific Indicators

- The use of numerous agent locations for no apparent reason to conduct transactions.
- Multiple low-value international funds transfers, possibly indicating a large amount of funds broken down into smaller amounts.
- Several customers request transfer either on the same day or over a period of two to three days to the same receipt.
- Customer does not appear to know the recipient to whom he or she is sending the transfer.
- Customer knows little about address and contact details for payee, is reluctant to disclose this information, or request a bearer instrument.
- Customer instructs that funds are to be picked up by third party on behalf of the payee.

### 4.4. Elements of Suspicious and Threshold Transactions

- Transaction deriving from:
  - the profile;
  - the characteristics; or
  - the usual transaction pattern of the relevant customer;
- Transaction reasonably suspected to have been conducted with the purpose of evading the reporting that must be conducted by the relevant reporting entity.
- Financial transaction conducted using fund alleged to be attributable to predicate offences.

### 4.5. Detection of Suspicious and Large Value Transactions

There are different indicators to detect suspicious transactions. Detection of suspicious transactions for the purpose of preventing money laundering and controlling terrorist financing, illegal activities, drugs and weapons supplies, etc. this document have been made and issued exercising the power conferred by Section 10 (1) (h) of Assets (Money) Laundering Prevention Act, 2008 (Second Amendment) as per Government of Nepal.

Based on this the company shall use the below information for detecting suspicious and large value transactions:

#### 4.5.1. Individual Transaction' History

i. Threshold based detection

ii. Situation/ activity based detection

iii. Misuse of Fund by or through individual/institutions

#### 4.5.2. Transaction information from other accounts in peer group

4.5.3. If company tends to suspect on conduction on any of the above mentioned activity

### **4.6. Terrorist Financing**

Terrorist financing provides funds for terrorist activity. The main objective of terrorist activity is to cause substantial property or human damage; or seriously interfering with or disrupting essential services, facilities or systems.

There are two main sources of terrorist financing:

- Financial support from countries, organizations or individuals, and revenue generating activities that may include criminal activities.
- The second source, revenue generating activities, may involve drug trafficking, human smuggling, theft, robbery and fraud to generate money.

Funds raised to finance terrorism usually have to be laundered and thus anti-money laundering processes in company & Remittance and other reporting industries are important in the identification and tracking of terrorist financing activities.

Company shall build measures to monitor, identify and report such funds received or sent using the Remittance system. I PAY REMIT shall take caution while doing transaction, or carrying Remittance activities if in any circumstances the name of any banned organization or individual (involved in terrorist activities) appears as payee/endorsee/applicant and report of such transaction as and when detected.

The Company shall endeavor to get the list of such organization/individuals to the best possible means or mechanisms.

## CHAPTER V

### MONITORING AND REPORTING SYSTEM

#### 5.1 Remittance Transaction Monitoring

The process (automated or manual) of monitoring transactions after the execution to identify unusual transactions, including monitoring single transactions as well as transaction flows, for subsequent review and, where appropriate, report to the authorities. The purpose of transaction monitoring is to provide ongoing identification of suspicious activity from customer transaction data.

Company shall review the customer Transaction on the basis of

- a) Paid and Unpaid Transaction Monitoring and
- b) Review of transaction and Revision of Risk Level.
- c) Monitoring the transaction status in system.

##### 5.1.1 Agent Transaction Monitoring

Money Laundering risk does not end after a agent has opened an account. To satisfy regulatory requirements and expectations as well as to protect the Company, the respective Unit must perform on-going monitoring of our Agent transaction. Compliance must ensure that the documents, data or information are retained are kept up-to-date and that the assessment of AML risk for the agent is appropriate. Company shall deploy the below mechanisms for ongoing transaction monitoring.

Company shall do the ongoing monitoring of Transaction based on Threshold Agent for both personal and non-personal Transaction

- Case logged by AML system
- Change of Transaction name
- Change of shareholders
- Change of signatories
- Change of Directors
- Activation of Document/ Where About Unknown (WAUN) Transaction.

- Remittance transaction reported as Suspicious
- It is apparent that the agent/customer has become a PEP
- Customer name has been alerted through public media, regulatory authority as investigation, Newspapers, Public media, Home ministry, UN sanction list, Nepal Police, Financial Information Unit (FIU), Tax Office, Commission for the Investigation of Abuse of Authority (CIAA), Tax, Revenue, Investigation, etc.

### **5.1.2 Remittance Review and Revision of Risk Level**

Ongoing review of Remittance is the process where I Pay Remit shall review all its Agents based on risk grading. For the purpose of agent review is to check the risk level assigned. For this I Pay Remit shall review the risk level of Level 2 Agent (Medium Risk Agents) Accounts in every 3 year and review of Level 3 Agent ( High Risk Agent) Accounts in every 1 year. After carrying out review of L2/L3 Accounts, the risk level shall be reduced to lower risk on the following conditions:

- In case of L2 Agent accounts, cumulative balance is less than prescribed threshold for both Personal and Non-Personal accounts for last 2 years
- Signatories/Directors/Head of the organization/ Shareholders/Beneficial Owners are no longer PEP
- Resident/ Operating Address is no longer fall under High Risk countries.
- Nature of Transaction is no longer fall under High Risk Transaction..

Joint approval of respective Segment Business Heads and Head Compliance shall be obtained for lowering of risk in all accounts.

### **5.2. Reporting Related to AML/CFT**

When detecting suspicious transaction or having the reasonable grounds to suspect the account transaction has derived from the illegal activity or in relation with money laundering, Compliance Department must report to FIU under the confidential mode.

I Pay Remit shall also generate TTR (Threshold Transaction Reports), STR (Suspicious Transaction Report) and other reports related to AML/CFT.

### **5.3 Content of Reporting**

#### a) Completeness

A single STR/TTR must stand-alone and contain complete information about the suspicion. A STR/TTR should provide a full picture of the suspicion itself as well as the objective facts and circumstances that gave rise to and support that suspicion. Where multiple transactions and/or behaviors are connected with a suspicion, a single report should be filed capturing all of these.

#### b) Narrative

The narrative portion of the report is most important. REs should perform proper analysis at their end regarding the STR/TTR and provide preliminary analysis report with relevant information and details as to why the reported transactions are suspicious.

#### c) Accuracy

It is imperative that factual information provided in the report is accurate. This is particularly true for identifiers such as names, citizenship numbers, registration numbers, etc. All spellings and transcriptions of identifiers should be double checked. A single inaccurate digit in a passport number or work permit, or a misplaced or transposed character in a name, can make the difference between a successful and an unsuccessful analysis. Identifiers for legal entities (e.g. company/business registration number, registered name of company) shall be exactly identical in every respect to those found on the official registration documents.

### **5.4. Retention of Records**

In terms of the operating procedures of the Remittance, records such as Agent Opening Forms, vouchers, ledgers, registers, etc., pertaining to Remittance Transactions for specified periods are required to be maintained.

To assist the authorities on investigation of cases of suspicious money laundering, it is essential that evidence of customer identification, address, transactions details are retained by the I Pay Remit as mandated by the regulators. Such records must be

archived in a secure area under the custody of a dedicated custodian. Access to such records must be made available only with due approval from Head Compliance.

- Records of every transaction undertaken for/by a customer must be retained for 5 years.
- Agent Opening / Closing forms/ Digital Certificate (DC) / Internet Remittance requests of the agents must be retained for 5 years from the date of closure.
- Documentary evidence of any action taken in response to internal and external reports of suspicious transactions must also be retained for 5 years.
- Where it is known that an investigation is ongoing, the relevant records must be retained until the authorities inform the Company otherwise.
- Audited reports or business documents must be retained for 5 years.
- Correspondent letter must be retained for 5 years.
- All the records should be maintained and saved for 5 years manually and in system.

## **5.5. Policy Compliance**

### **5.5.1. Employee and Agent Training Program**

Training shall be provided to business units that offer products and services that are subject to the legislative requirements. Staff involved in customer facing areas, remittances, etc. of I Pay Remit shall receive periodic training and reminders on the detection and reporting process for suspicious activities. Communication of changes to AML/CFT legislation or any emerging risks are communicated to the relevant staff. Training workshops conducted by Regulator should be attended by compliance department.

In addition to the above, Human Resource Department shall make sure that the training on AML Policy will also be provided to all the staff of I PAY REMIT using internal or external resources and as and when there are changes in AML Policy/procedures or there are developments in the AML trends worldwide.

### **5.5.2 Amendment to the policy**

NRB and FIU may issue the AML related circular/directives from time to time and the KYC/AML/CFT acts and laws of the country shall form integral parts of this

policy. If any section/sub-section/clause of this policy contradicts with the country's laws, FIU/NRB's directives, circulars; the latter shall be valid to the extent of contradiction.

This policy is subject to review at least annually or as required for updates in the terms or any clause of the policy. There shall be a separate AML/KYC procedure formulated by I Pay Remit.

### **5.5.3 Compliance Measurement**

MLPO or the designated officer will verify compliance to this policy through various methods, using various tools, reports, internal and external audits, and feedbacks to the policy owner. I Pay Remit auditors and internal compliance departments shall conduct programs of audit and compliance testing of this policy and operational procedures applicable to AML. The frequency and scope of the audits and compliance tests are determined through a risk-based approach, where higher risks to I PAY REMIT are audited and tested more frequently. The audit and compliance programs shall be approved by senior management.

### **5.5.4 Exceptions**

Any exception to the policy must be acknowledged by MLPO and approved by the I Pay Remit management.

### **5.5.5 Non-Compliance**

An employee found to have violated this procedure may be subject to disciplinary action, as per the provisions in the prevailing I PAY REMIT Employee Policy.

### **5.5.6 Repeal and Saving**

- Anti-Money Laundering Policy, 2008, is hereby repealed.
- Activities carried out related AML monitoring, implementation, reporting etc, under Anti Money Laundering Policy, 2008 shall be considered as done under this policy.

## **5.6 Reporting through goAML Software**

The TTR and STR report has been submitted to FIU under the guidelines of NRB through the goAML reporting software provided by Nepal Rastra Bank.



## CHAPTER VI

### BARRIERS FOR TRANSACTIONS

#### 6.1 Barriers for Transactions

There are certain criteria for the barrier of the transaction process if not presented with the required valid documents. The nature of transactions are mentioned as:

- Not presenting KYC as required
- Documents submitted but not sufficient for verification
- Not eligible to make transaction concerning above points and inform to FIU whether or not the transaction is made
- If the previous transaction's customer tends to not meeting and providing the required documents for verification
- If the transaction is made with the purpose of donation to church or temples that have no legal existence or unregistered.
- PEPs
- PEP Close Associate
- Arms, Defense, Military
- Non-Government Organizations
- Embassies/Consulates

#### 6.2 Restricted Transaction made in the category of customers listed as:

- Non-account Customers
- Offshore Customer
- Shell Bank
- Atomic Power
- Extractive Industries
- Precious Metals and Stones
- Unregulated Charities
- Regulated Charities
- Red Light Business/ Adult Entertainment / Gambling
- Virtual Currencies

## CHAPTER VII

### MISCELLANEOUS

#### 7.1 Correspondent and Shell Company

##### 7.1.1 Correspondent company

I PAY REMIT shall implement risk based due diligence procedures that include, but are not limited to, the following – understanding the nature of the correspondent’s business, its license to operate, the quality of its management, ownership and effective control, its AML Policies, external oversight and prudential supervision including its AML/CFT regime.

Additionally, ongoing due diligence of correspondent Principal Remittance Company shall be performed on a regular basis or when circumstances change. Remittance policies also ensure that we do not offer ‘payable through Remittance’. All correspondent Remittance relationships are approved by senior management of the Company.

##### 7.1.2 Shell Company

I PAY REMIT shall not conduct business with shell company or Shell Principal Remittance Company. Our policies and procedures shall prohibit offering services to shell company and shell Remittance Company.

#### 7.3. Miscellaneous Grounds for Suspicion

- If any of the transaction is not found reasonable or is found to have been conducted with irrelevant party or where the transaction has no justifiable purpose.
- If it is evident that the asset is earned from extortion, coercive donation collection or from any forcible means to compel one to pay amount or asset.
- If it is evident that the transaction is related to any person who is involved in suspicious transaction, likely to promote money laundering, terrorist or any other criminal activities or the transaction that appears to be unnatural or suspicious in any manner.
- If same address or telephone number/mobile number is provided for different unrelated customers.

- If same ID number is provided for different unrelated customers.
- If there is cross transaction between customers who are not related with each other or any individual transmits to receives amount from unrelated person or business institution's account.
- If there is suspicion that any transaction is aiding criminal activities or receiving amount from such activities.
- If anyone denies providing identity information or clear justification of the transfer through there are sufficient grounds to know such information.
- Any other transaction the reporting institution finds the grounds for suspicious transaction reporting as per the prevailing law.
- Transactions status in the system should be displayed recorded with all the information of sender and receiver.
- Notification or alert messages should be received by compliance and operations units if the transaction with the same sender or receiver meeting the threshold amount or suspicious including their all information.

