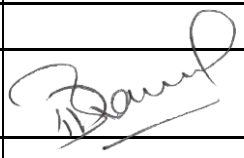
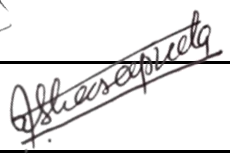
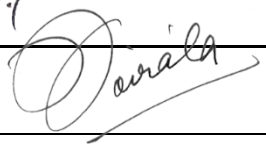
AML/CFT POLICY

ESEWA MONEY TRANSFER PVT. LTD.

AML/CFT Policy 2022-2023	Particulars	Remarks
	Version	(3.0)
	Version Date	November 2022
	Approver(s)	Management/BODs
	Approved Date	November 22, 2022
Approvers (BOD Name)	**Signature**	
Biswas Dhakal		
Subhas Sapkota		
Daniel D Shrestha		
Ajesh Koirala		

Revision History

Date	Version	Description	Prepared by	Approved by
November 2019	1.0	Document initiation	Group Legal	BOD
February 2020	1.0	Reviewed	Indra Basnet	BOD
December 2021	2.0	Reviewed & updated	Indra Basnet	BOD
November 2022	3.0	Reviewed & updated	Rakshya Giri	BOD

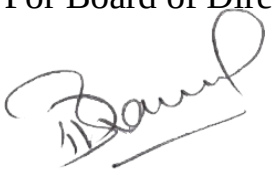
Declaration:

We, at Esewa Money Transfer Pvt. Ltd., know the portliness of Money laundering and its effect globally and for that, we fully cooperate with the Government of Nepal, Central Bank of Nepal (NRB), and all the component government agencies fighting against it. We understand and have made our AML/CFT policy as per the laws, Directives, Circulars, and Rules and Regulations of the Nepal Rastra Bank.

We as corporate citizens and the financial institutions will take all necessary steps to ensure that the policies of AML/CFT as directed by the Central Bank of Nepal and with the international standards as formulated from time to time shall have complied within the right earnest.

Regards,

For Board of Directors



Biswas Dhakal
President/BOD

Message to all Employees and Esteemed Partner/Agents

Money Laundering & Terrorist Financing has been identified as a major threat to the international financial services community. Many governments have passed legislation designed to prevent these, which imposes certain requirements upon institutions registered in their jurisdiction. These legislations are a statement of the minimum standards to be adopted by all registered financial institutions operating in their jurisdiction.

As a major player in the Inward Remittance business in Nepal and as a responsible corporate citizen of the country, it is incumbent on us to comply with the regulations of AML in force and assist our government and governments across the globe in preventing the process of Money Laundering in every possible way.

Esewa Money Transfer has adopted best practices in the industry for AML & CFT Policy and Procedures. Esewa Money Transfer has a responsibility to help fight money laundering and terrorist financing. As a company operating within a boundary as a receiving agent, we can be one of the targets of would-be money launderers & terrorist financiers. We hope that you too will share this commitment to prevent our products and services, as well as your business, from being used for illegal purposes. Money laundering and terrorist financing is a crime that can lead to losses, fines, seizure of accounts, cancellation of license, individual imprisonment as well as damage the reputation of both of our businesses if we do not take care.

It is our sincere appeal to all staff members and our Partner Associates to familiarize themselves with the AML/CFT & KYC provisions and ensure complete compliance in the conduct of Inward Remittance Activity. Working together, we can help prevent this illegal activity from occurring.

Compliance Dept., Management

& Board of Directors

Esewa Money Transfer Pvt. Ltd.

Table of Contents

Chapter:1
INTRODUCTION

a. This Anti-Money Laundering and Anti-Terrorist Financing Policy (Policy) of Esewa Money Transfer Private Limited, Nepal (Esewa Money Transfer) has been developed keeping in consistency with the Asset (Money) Laundering Prevention Act, 2008 issued by Nepal Rastra Bank (Central Bank of Nepal).

b. The aim of this Policy is to facilitate compliance by Esewa Money Transfer by explaining the duties and responsibilities of Esewa Money Transfer with respect to the implementation of the AML/CFT measures to deter, detect and disrupt money laundering/terrorism financing activities under the Asset (Money) Laundering Prevention Act, 2008(AMLPA).

c. The Board of Directors has the ultimate responsibility to ensure the company's compliance with the provisions of AMLPA. An independent function will be established to check the compliance status.

d. The policy should be reviewed regularly and updated as necessary based on any legal/regulatory or business/operational changes, such as amendments to existing AML/CFT rules or regulations.

1.1 What is Money Laundering?

Money Laundering is any act designed to hide the source, destination, ownership, or control of funds that may have been derived from illegal activity, or are intended to be used for illegal activity.

Some of the monetary activities that are considered illegal is derived from includes:

a. Terrorism, piracy and kidnapping

b. Drugs

c. Illicit dealing in fire-arms and ammunition

d. Bribery, embezzlement, and damage to public property

e. Fraud, breach of trust and related offences

f. Offences committed in violation of the environmental laws

g. Any other related offences referred to in international conventions to which the State is a party

1.2 Definitions under Asset (Money) Laundering Prevention Act, 2008

"Assets Supposed to Have Laundered" means the act – in case anyone, directly or indirectly, earns from tax evasion or terrorist activities or invests in such activities or acquires, holds, possesses or utilizes assets by committing any or all offences stipulated as follows and in case assets acquired, held or accumulated from investment of such assets is possessed, held or used, utilized or consumed or committed any other act so as to present such assets as legally acquired or earned assets or conceals sources of origin of such assets or assists anyone to transform, conceal or transfer such assets with an objective of avoiding legal actions to the person having such assets:

a. Offences under the prevailing arms and ammunitions laws.

b. Offences under the prevailing foreign exchange regulation laws.

c. Offences of murder, theft, cheating, forgery documents, counterfeiting, kidnap or abduction under the concerned prevailing laws.

d. Offences under the prevailing drug addiction control laws. cooperatives

e. Offences under the prevailing national park and wild animal's conservation laws.

f. Offences under the prevailing human trafficking and taking of hostages control laws.

g. Offences under the prevailing cooperatives laws.

h. Offences under the prevailing forest laws.

i. Offences under the prevailing corruption control laws.

j. Offences under the prevailing bank and financial institution laws.

k. Offences under the prevailing banking crime and punishment laws.

l. Offences under the prevailing ancient monuments conversation laws.

m. Other offences that Government of Nepal prescribes by publishing in the Nepal Gazette.

Clarification: For the purpose of this section, in case anyone has committed any act supposed to be an offence under the following conventions or provided or collected any money by any means for murdering or physically disabling any other knowingly or with grounds that such money is being used for committing such offence, he shall be supposed to have invested in terrorist activities:

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

b. Hague Convention for the Suppression of Unlawful Seizure of Aircraft, 1970,

c. Montréal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 1971,

d. Convention on the Prevention and Punishment of Crime against Internationally Protected Persons Including Diplomatic Agents, 1973,

e. International convention Against the Taking of Hostages, 1979,

f. SAARC Regional Convention on Suppression of Terrorism, 1987,

g. Any Convention against Terrorist Activities to which Nepal is a party.

1.3 Different stages involved in money laundering

a. Placement:

The first stage is successfully disposing of the physical cash received from illegal activities. Money laundering is a "cash-intensive" business, generating vast amounts of cash from illegal activities. The monies are placed into the financial system or retail economy or are smuggled out of the country. The aims of the launderer are to remove the cash from the location of acquisition so as to avoid detection by the authorities and to then transform it into other asset forms.

b. Layering:

In the course of layering, there is an attempt at concealment or to disguise the source of ownership of the funds by creating complex layers of financial transactions also designed to disguise the audit trail and provide anonymity. The purpose of layering is to disassociate the illegal monies from the source of the crime by purposely creating a complex web of financial transactions aimed at concealing any audit trail as well as the source and ownership of funds.

c. Integration:

The final link in money laundering process is called the integration stage. It is this stage at which the money is integrated into the legitimate economic and financial system and is assimilated with all other assets in the system. Integration of the "cleaned" money into the economy is accomplished by the launderer making it appear to have been legally earned. By this stage, it is extremely difficult to distinguish legal and illegal wealth.

1.4 Penalty of Money Laundering

As per Sub-Section 30 of the Assert Money Laundering Act 2008,

a. Anyone committing offence under section-3 shall be punished as follows, in Accordance with the degree of offence committed:

i. Fine equal to the amount involved in the offence or imprisonment from one year to four years or both punishments to any person or staff of a bank, financial institution or

nonfinancial institution who has committed offence or in case such staff is not identified for the person working as chief at the time of committal,

ii. In case an office bearer, chief of staff of a bank, financial institution or non- financial institution or public servant has committed offence, ten percent more than the punishment written in clause (i).

b. The person assisting or provoking to commit fraud or causing to commit offences under this Act shall be punished half of the offender.

1.5 Implementation of the AML/CFT Measures

In carrying out money transfer services activities, Esewa Money Transfer is required to establish and implement effective AML/CFT measures in order to mitigate the risk of money services business transactions being carried out for money laundering, terrorist financing and other illegal purposes. These AML/CFT measures include the following:

a. **Customer Due Diligence (CDD or Know Your Customer, KYC):** Conduct of customer due diligence to identify and verify the customer who Esewa Money Transfer is dealing with;

b. **Record Keeping:** Maintenance of relevant records and documents relating to transactions undertaken by Esewa Money Transfer;

c. **Ongoing Monitoring of Transactions:** Ongoing monitoring of transactions with customers to ensure information maintained by Esewa Money Transfer is current and relevant to support detection of suspicious transactions; and

d. **Reporting of Suspicious Transactions:** Submission of suspicious transaction reports to the Financial Information Unit in Nepal Rastra Bank when Esewa Money Transfer has any suspicion of a transaction being associated with money laundering, terrorism financing or other illegal activities.

Chapter:2
CUSTOMER DUE DILIGENCE (CDD) OR KNOW YOUR CUSTOMER (KYC)

2.1 Customer Due Diligence (CDD)

a. **Customer due diligence (CDD):** is about knowing the customer, who Esewa Money Transfer is dealing with, be it an existing or a new customer.

b. The conduct of effective CDD will enable Esewa Money Transfer to detect possible transactions for money laundering, financing of terrorism or other illegal activities at the point of customer contact, hence, and safeguarding Esewa Money Transfer from the abuses of financial crimes and other unlawful activities.

c. An extra measure applied to know more about the customer and their business activities is known as Enhanced Due Diligence. This includes gathering of additional information by Esewa Money Transfer which includes but is not limited to:

- The customer's local and overseas client(s)
- Countries of business involved
- Review of documents related to trade like statements, invoices, shipping documents, site visits
- Frequency & volume of transactions
- Beneficiary nationality
- Relationship between remitter and beneficiary

2.2 Requirements under Customer Due Diligence (CDD)

a. Esewa Money Transfer shall perform the following steps to conduct a comprehensive CDD before undertaking a transaction with the customer:

- Sight the Original Identification Documents of All Customers following original identification documents of all customers, regardless of the amount transacted.
- For Individual Customer Citizenship certificate or driving license or passport for Nepali citizen. Passport or Work Permit or other valid official identification documents for foreigner.

b. Notice to Customer for Production of Relevant Identification Documents:

- For the purpose in above paragraph, Esewa Money Transfer shall display up in a conspicuous position a notice in the format below informing its customers to produce the relevant identification documents:

Notice to Customer:

Please produce your identification document before making a transaction as required under the Asset (Money) Laundering Prevention Act, 2008.

c. Verify with the UN Sanction List: Verify that the customer is not listed in the United Nations Security Council Resolution (UNSCR) list of terrorists where there are existing sanctions against individual and entities related to. Esewa Money Transfer shall keep itself updated by downloading the updated and consolidated United Nations Sanction List from http://www.un.org/sc/committees/1267/pdf/AQList.pdf.

d. Verify with the Local Sanction List: Esewa Money Transfer should also refer to the list issued by regularities authorities of Nepal.

e. Customer is listed in any of the lists mentioned in Paragraph-2.2 (c) and (d) above: Esewa Money Transfer must reject the transaction and submit a suspicious transaction report to the Financial Information Unit in Nepal Rastra Bank on the ground that the transaction is terrorist-related.

f. Note down the Particulars and Make Duplicate of the Original Identification Document: Esewa Money Transfer must note down the particulars of the customer and make a duplicate copy of the original identification document for every remittance transaction payment.

2.3 System Capabilities

Esewa Money Transfer is carrying out remittance business by using the remittance system "Esewa Remit" web-based remittance software, developed by Inficare. Salient features of the system are as follows:

- **"Esewa Remit**", the remittance system, is capable to verify the identity of the customer performing the transaction over the limit of NPR. 1,000,000/ (One Million Only).
- The remittance system is featured as to generate an exception report for remittance transaction value over NPR. 1,000,000/-.

2.4 Situations Requiring Enhanced Due Diligence (EDD) on Customers

In the following certain situations, regardless of the amount transacted, Esewa Money Transfer is required to perform additional steps to conduct Enhanced Due Diligence (EDD), in addition to the CDD process being undertaken:

a. Esewa Money Transfer will conduct enhanced due diligence in cases where it is required under the provision of Law or regulations or when there is a perception of high risk of money laundering or terrorist financing.

b. High Risk Customer: When Esewa Money Transfer is dealing with a "high risk" customer. Examples of a "high risk" customer are:

- High net worth individuals.
- Non-resident customers.
- Unrelated Sender and Receiver.
- Customers from locations known for their high rates of crime (e.g., drugs producing; trafficking and smuggling).
- Politically exposed persons who are being or have been entrusted with prominent public functions, such as heads of state or government, senior politicians, senior government officials, judicial or military officials and senior executives of public organizations.
- Business/activities identified by the FATF as of higher money laundering and financing of terrorism risk such as activities related to casino, dealers in precious metals and stones, trust and company service providers (TCSPs) and real estate agents.

c. When there arises any doubt over transactions which may appear to be unusual or do not have any apparent economic purpose. Examples of transactions that may trigger suspicion are listed in Annexure-A.

d. **Monitoring of Transactions Effective:**

KYC procedures require continuous monitoring of our customer base and its normal behavior to reduce risk. High-risk transactions (classified based on country of origin, fund sources, etc.) or activities (such as complex or unusually large transactions and those with no visible lawful purposes) should undergo extra scrutiny. Company can set thresholds for transaction amounts that warrant enhanced due diligence.

2.5 Enhanced Due Diligence (EDD) on Customers

The measures for Esewa Money Transfer to conduct EDD include, but are not limited to the followings:

a. Obtain more detailed information from the customer, in particular, on the purpose of transaction and the source of funds.

b. Make duplicate copy of the original identification documents(s), even if the amount of the transaction is less than the respective thresholds set in Paragraph- 2.2(f) above.

c. Obtain approval from the senior management, such as the Chief Executive Officer, before establishing the business relationship or transacting with the customer.

d. When a service is provided to minor, normal identification policies must be followed along with establishing the identity of the legal parent(s) or guardian(s).

e. Esewa Money Transfer will not conduct the transaction in case of non-face- to-face business as well as if the representative will act on behalf of third party.

2.6 Failure to Conduct CDD or EDD on Customers

a. Esewa Money Transfer must not continue the transaction if it fails to conduct proper CDD and/or EDD on the customer.

- Before establishing drawing arrangements with overseas Correspondents/ Agents for making payments of remittance drawn to them, due diligence is to be ensured.
- To executive drawing arrangements, senior management approval must be obtained on being satisfied about the nature of the business of the correspondent/agent through collection of information as per Annexure-C, which is to be reviewed from time to time.
- **Customer Acceptance Policy (CAP):** Must be clear with explicit criteria. Perform due diligence with background checks to ensure that customer/entity is using their real name and not involved in terrorism or other illegal activities by checking valid photo ids.

b. **Customer Identification Procedures (CIP**): At every stage of the company relationship: carrying out a transaction, resolving doubts about the authenticity of previously obtained identification, etc. Identify and verify all customers' identities and purposes (using reliable, independent data, information, and/or source documents) must be clearly outlined and performed to the Esewa Money Transfer's satisfaction.

2.7 Payer Due Diligence

a. Before establishing drawing arrangements with overseas Correspondents/Agents for making payments of remittance drawn to them, due diligence is to be ensured.

b. To executive drawing arrangements, senior management approval must be obtained on being satisfied about the nature of the business of the correspondent/agent through collection of information as per Annexure-C, which is to be reviewed from time to time.

c. **Customer Acceptance Policy (CAP):** The Company's Customer Acceptance Policy (CAP) lays down the guidelines for acceptance of potential customers and ensures that only those customers whose identity and purpose of performing transactions can be duly established and verified as legitimate are accepted.

The customer registration procedure is mandatory for all transactions. The Company shall conduct enhanced due diligence of any person applying to do business with it. The

Compliance Officer shall obtain satisfactory evidence of the identity and legal existence of persons conducting transactions on the basis of reliable documents or other resources.

No registration or transaction is to be carried out:

• If customer does not provide document, information and details required for customer identification and verification and customer due diligence.

• If the documents, information and details provided appear conflicting to the identity of the customer.

• The transaction is accompanied with incomplete or otherwise misleading documents or information.

• If the persons having relationships with sanctioned/banned persons or entities such as individual terrorists, terrorist group or terrorist organizations etc.

• The transaction is related with shell entity/shell bank/virtual currency/crypto-currency.

2.8 Customer Identification Procedures (CIP)

At every stage of the company relationship: carrying out a transaction, resolving doubts about the authenticity of previously obtained identification, etc. Identify and verify all customers' identities and purposes (using reliable, independent data, information, and/or source documents) must be clearly outlined and performed to the Esewa Money Transfer's satisfaction.

This means that staff must conduct the following:

a. Physically inspect the original of the customer's personal identification document;

b. Check the customer is the person referred to in the identification document;

c. Take reasonable steps to ensure that the customer's personal identification document is valid and genuine.

d. Inspection of all documents should be carefully done. The photo, name, signature, expiry date, etc., given in all the documents and papers should be carefully tallied.

Chapter: 3
RECORD KEEPING REQUIREMENTS

3.1 Record Keeping

An efficient records management program is necessary for organizations to proactively and progressively manage all data, media and information. Policies and procedures set standards and serve as evidence of management's support and investment in a compliant records management program. These procedures should be accessible and communicated clearly. Record retention should be practiced consistently throughout an organization. When employed properly, they work in conjunction with an organization's Business Continuity Plan and Disaster Recovery Program.

3.2 Objective of Record keeping

The objective of record keeping is to ensure that an exchange house shall be able to provide the basic information about the customer and to reconstruct the transactions undertaken at the request of the relevant authorities at any given time. Esewa Money Transfer has maintained all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

3.3 Information Requirements

a. Esewa Money Transfer is required to keep relevant records for each transaction of its money services business. The records maintained must enable Esewa Money Transfer to establish the history, circumstances and reconstruction of each transaction.

b. The receipts issued for each transaction should contain the following details, at minimum:

- The name, address and contact details of sender,
- Source of Income,
- Relationship between sender and receiver,
- Purpose of remittance
- Valid Identification No.
- Receipt serial number,
- Date of transaction,
- The name of sender,
- The name of beneficiary and contact details,

- The amount of funds to be remitted in foreign Currency and its equivalent amount in Nepalese Rupees to be received by the beneficiary,
- The origin and destination of fund transfers, and
- Other relevant document(s) supporting the transaction, including bank-slips.

c. Esewa Money Transfer shall also keep records of the customer's particulars as stated above respectively.

3.4 Formats and Retrieval of Records

a. The records must be maintained in a form that will enable the creation of an audit trail on individual transactions that are traceable by the Nepal Rastra Bank and the relevant law enforcement agencies.

b. The records can be kept:

- By way of original documents;
- By way of duplicate copies of the original documents;
- In scanned form;
- In computerized or electronic form;
- On microfiche.

3.5 Period of Retaining Transactions of Records

a. The Nepal Rastra Bank requires Esewa Money Transfer to keep records for a period of five years after a transaction has been completed.

b. However, if the records are required for prosecution or criminal investigation purposes, Esewa Money Transfer may be required to keep the record longer than the period stated above or until such time the records are no longer needed.

c. If Esewa Money Transfer has provided the records to Nepal Rastra Bank or to a law Enforcement agency, it will no longer have an obligation to keep those records as they are not within the possession of Esewa Money Transfer.

Chapter: 4
ONGOING MONITORING OF TRANSACTIONS AND CONFIDENTIALITY

4.1 Ongoing Monitoring of Transactions

a. Esewa Money Transfer shall conduct ongoing monitoring on its transactions and regular customers to ensure that the records / information maintained are up-to- date to facilitate

the detection of any suspicious transaction that may appear to be inconsistent with the expected pattern of the customer.

b. As there are unlimited types of transactions that a money launderer or a terrorist Financier may use, it is difficult to define a suspicious transaction. However, in most of the cases, a suspicious transaction will be one that is inconsistent with a customer's known, legitimate business or personal activities.

c. In this regard, a few criteria to detect suspicious transactions are listed in Annexure- A. These are not intended to be exhaustive and only provide examples of the most basic way by which money may be laundered or financed for terrorism.

d. However, any transaction that matches the above criteria should be subjected to higher scrutiny by the Compliance Officer (CO) who should evaluate whether a suspicious transaction report should be submitted to the Financial Information Unit in Nepal Rastra Bank.

4.2 Maintain Confidentiality and Secrecy

The above reviews are done as a part of the daily functions of Esewa Money Transfer. It should be kept in mind that all exceptions may not be suspicious. Also, Esewa Money Transfer officials should be very much cautious in dealing with customers. They should perform the job in a manner that do not make any panic and do not disclose any information to any person. No officials at any level shall divulge any information regarding the reported unusual or suspicious transactions or any other information, at any stage to its customer or any other person, so that the investigation procedure is hampered or influenced adversely. Except for the purposes permitted under AMLPA.

4.3 Blacklisted Entities and Individuals

a. The Compliance Department at the Head Office shall continually obtain information of Black Listed Entities and Individuals from the regulatory authorities and international agencies and update the same in the system. Every transaction received in Esewa Money Transfer goes through the screening process. Esewa Money transfer uses following sanction screenings.

- OFAC (Office of Foreign Assets Control)
- PEP (Politically Exposed Person)
- UKHM – HMT Financial Sanction List
- UN (United Nation Sanction List)
- CAD (Credit Administration Department)
- CIB (Central Investigation Bureau)
- EU (European Union)
- NS – PLC (Non-SDN Palestinian Legislative Council)
- NS – PLC – Aka

- NS – PLC – Add

b. Blacklist scanning function shall be done real time and centralized at the Head Office. All transactions irrespective of the amount shall be scanned against the Blacklist database. If there is any name match of the customer beneficiary, the transaction shall be immediately suspended and an alert sent to the AML & CFT Department and the respective Branch. The customer beneficiary details of the suspended transaction shall be checked against the blacklist database and if different, the suspension shall be revoked. If there is an exact match, the transaction shall be blocked and reported to the local regulatory authority.

c. The FATF recommends that special attention should be given to business relations and transactions with persons including companies and financial institutions from the "Non-Cooperative Countries and Territories" (NCCT).

d. The Compliance Department at the Head Office shall furnish available details to the Central Bank of Nepal or any other regulatory authority law enforcement authorities for any request for information within a reasonable period of time.

e. In case there is any doubt that a transaction is meant for a terrorist organization or terrorist purposes, Agent shall freeze the transaction and inform the Central Bank of Nepal in writing immediately.

4.4 Politically Exposed Persons (PEPs)

Politically exposed persons (PEPs): Present potentially higher risk situations. Additional due diligence is required when dealing with these people. Politically exposed persons are understood to be persons entrusted with prominent public functions, their immediate family members or persons known to be close associates of such persons. Public functions exercised at levels lower than national level should normally not be considered prominent however where their political exposure is comparable to that of a similar position at the national level, they should be considered on a risk sensitive basis whether they should also be considered a PEP. The actual definition of a PEP found in the 3rd Anti-Money Laundering Directive is as follows:

a. Heads of state, heads of government, ministers and deputy ministers

b. Members of parliament

c. Members of supreme courts, of constitutional or other high level judicial bodies

d. Members of courts of auditors or of the boards of central banks

e. Ambassadors, charges d'affaires and high-ranking officers in the armed forces

f. Members of the administrative, management or supervisory bodies of state-owned companies and in each instance include the following:

g. The spouse or any partner equivalent to a spouse

h. The children and the children's spouses

i. Parents

j. Any close associate who is defined as any person who is known to have a joint beneficial ownership in a legal entity with a person listed above or has sole beneficial ownership in a legal entity that is known to have been established for the benefit of a person listed above.

Chapter: 5
SUSPICIOUS TRANSACTIONS AND IT'S MECHANISM

5.1 Recognition and Reporting of Suspicious Transactions

There is no clear regulatory pronouncement as to what constitutes a suspicious activity but a suspicious transaction will often be one which is inconsistent with that customer's/counterparty's known legitimate business or personal activities or with the normal business for that type of account. Suspicious activity can occur either in the negotiation stages with a prospective customer in order to commence a business relationship, or at the outset of the client relationship or even long after the relationship has been initiated.

5.2 Obligation for Reporting of Suspicious Transactions

Esewa Money Transfer is obligated to submit a suspicious transaction report to the Financial Information Unit in Nepal Rastra Bank when any of its employees/payout agents suspect or have reason to suspect that the transaction involves proceeds from an unlawful activity, or the customer is involved in money laundering or terrorism financing.

5.3 When to Report Suspicious Transactions

Esewa Money Transfer shall consider submitting a suspicious transaction report when:

a. Unable to complete the CDD process on any of its existing or new Customer who is unreasonably evasive or uncooperative.

b. Any of its customer's transaction or attempted transaction fits Esewa Money Transfer's criteria.

5.4 Mechanism for Reporting of Suspicious Transactions

The mechanism of reporting Suspicious Transaction are:

a. All officials of Esewa Money Transfer must be alert to transactions that are inconsistent with the customer's CDD / KYC information.

b. If any unusual transaction is found, then the staff who has noticed it will immediately fill-up the "Suspicious Transaction Report Form" (refer to Annexure-2) and submit to the CO.

c. The CO will evaluate the reported incidence properly in the light of all other relevant information and record in writing with reasons in details whether the transaction is connected with money laundering or terrorist financing or not.

d. If the reported issue does not appear to be connected with money laundering or terrorist financing, then the CO will close the issue at his end after putting his comments on the STR form.

e. If the reported issue appears to be connected with money laundering or terrorist financing, then the CO will submit the Suspicious Transaction Report to the concerned regularity authorities through any of the following modes:

- Mail: Director, Financial Information Unit Nepal Rastra Bank, Kathmandu, Nepal (to be opened by addressee only)
- Fax: +97714410159

f. For this purpose, the CO has necessary independence to report the suspicious transaction, where obtaining approval from its senior management or Board of Directors will not be necessary.

g. Additionally, the CO is authorized to cooperate with the Financial Information Unit in Nepal Rastra Bank, including providing additional information and documents as the Bank may request; and to respond promptly to any further enquiries relating to the suspicious transaction report.

h. **STR Register**: All investigation issues must be documented in a register. The register should include the investigation issue and the rationale for the disposition of the case. In addition, any unusual activity for which decision was taken not to file a STR should also be documented in the register.

5.5 Red Flags – Possible Suspicious Fraud Activity Signals

The following are **'red flags'** and **'frauds'** that can indicate suspicious activity. The examples do not necessarily represent reportable events but they do suggest situations that may be indicative of activity that should be followed up and clarified:

a. General Typologies

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the firm's policies relating to the deposit of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the NPR 1,000,000/- government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non- cooperative country or territory by the FATF.
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer's account shows numerous currency or cashier's check transactions aggregating to significant sums.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for the purpose of purchasing a long -term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.

- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation Stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.
- The customer engages in a transaction which contains a misrepresentation of the price, quantity or quality of imports or exports.
- The customer carries out fictitious trade activities through front companies.

Chapter:6
ORGANIZATIONAL STRUCTURE AND MANAGEMENT

6.1 Organizational Structure

Esewa Money Transfer shall designate a staff at the senior management level as its Anti-Money Laundering Compliance Officer (CO). The CO shall implement and enforce corporate-wide anti-money laundering and anti-terrorist financing policies, procedures and measures and will report directly to the Chief Executive Officer.

6.2 Anti-Money Laundering Compliance Officer (CO)

Esewa Money Transfer has appointed Ms. Rakshya Giri as its MLRO whose primary responsibility is to ensure the effective implementation and enforcement of the policies set forth in Esewa Money Transfer's Anti-Money laundering Compliance Manual.

a. The CO will be the single point of reference for the Financial Information Unit in Nepal Rastra Bank on matters relating to AML/CFT.

b. The CO must be fully familiar with the AML/CFT requirements and have the ability to evaluate and establish the case for a suspicious transaction, and ensure that the suspicious transaction report submitted to the Financial Information Unit in Nepal Rastra Bank meets the expectation of the Bank.

c. The name and contact details of the CO shall be informed in writing to the Financial Information Unit in Nepal Rastra Bank on the appointment or change in the appointment of the CO.

6.3 Responsibilities of the Anti-Money Laundering Compliance Officer (CO)

Key Responsibilities of Compliance Officer

1. One of the major responsibilities of CO is to report any suspicious transactions to the Financial Information Unit in Nepal Rastra Bank. In relation to this, the CO must ensure that:

   a. All the Staffs/agents involved in conducting or facilitating customer transactions are aware of the suspicious transaction reporting procedures established within Esewa Money Transfer.

b. The mechanism for channeling the internally generated suspicious transaction report from the respective staff to the compliance officer is secured and that information is kept confidential.

c. All internal suspicious transaction report received from the head office, branches and the agents are appropriately evaluated, and submit the suspicious transaction report to the Financial Information Unit in Nepal Rastra Bank within the next working day, from the date the compliance officer establishes the suspicion. In the case where the CO decides that there are no reasonable grounds for suspicion, he should document his decision and ensure that it is supported by the relevant documents.

d. A complete file on all internally generated suspicious transaction reports and the supporting documentary evidence is maintained, regardless that such report has been submitted to the Financial Information Unit in Nepal Rastra Bank.

2. Ensure that internal AML/CFT policies are properly developed and reflect the nature of the activities of Esewa Money Transfer.

3. Ensure effective monitoring of Esewa Money Transfer's compliance with the AML/CFT requirements, particularly on CDD, record keeping and ongoing monitoring of customer and transactions.

4. Ensure timely escalation of any material breaches or operational lapses relating to the implementation of AML/CFT measures to the Board.

5. Adequate staff/agents training and awareness on the Esewa Money Transfer's internal AML/CFT measures and procedures with relevant guidelines relating to AML/CFT compliance.

6.4 Risk Assessment and Management

Keeping in view the objectives of National Money Laundering/Financing of Terror Risk Assessment Committee of Government of Nepal, we have adopted a risk-based approach, assessment of risk and put in place a system which would use that assessment to take steps to effectively counter money laundering/terrorism finance so as to make AML/CFT regime more robust for which purpose we shall allocate resources more judicially and efficiently. Each customer will be assigned and appropriate risk rating based on his/her profile and enhanced due diligence measures will be applied to high-risk customers. We shall identify and assess money laundering/terrorism finance risk for customers, countries and geographical areas as also for products/services/transactions/delivery channels etc.

Keeping the above in view, we have put in place an effective internal control system to:

a. Assess each customer for the risk, assign a risk rating and accordingly undertake due diligence;

b. Approve transactions;

c. Monitor transactions both online and off line;

While the online monitoring will be through the system control, off line will be by deputing senior officials to the branches to conduct a surprise inspection. This will be in addition to the Concurrent Audit System already in place. The staff will be trained and refresher courses will be conducted to enable them update their knowledge. The risk profiles of the customers will be reviewed and updated from time to time.

The mandatory Concurrent Audit is entrusted to firms of outside Chartered Accountants with instructions to check all the transactions and to ensure that the transactions are undertaken in compliance with the anti-money laundering guidelines and necessary reports are furnished to the authorities concerned in time, including but not limited to the NRB and the FIU. The same has been working satisfactorily.

We also have a separate Audit Department at Head Office with set ups at regional levels. The department is entrusted with carrying out of Inspection of the branches on a monthly basis. The staff inspecting the branches is rotated so that the same Inspector is not deputed for inspection of the same branch i.e., branches and inspectors are rotated. Further, Inspection of the branches in one Region by Inspectors from other Regions is also done frequently so that the inspection is more effective. Audit Programme/Schedules are kept confidential so as to avoid any tip off. Compliance on the lapses, if any, recorded by the concurrent auditors shall be put up to the top management. We will also ensure to obtain from the Statutory Auditors a certificate on compliance with the KYC/AML/CFT guidelines at the time of preparation of our Annual Report and keep it on record.

6.5 Review and Auditing of Anti-Money Laundering Program

a. A robust AML & Compliance program shall be complete where a periodic review to assess the adequacy of the policies & procedures, compliance officer's functions and other controls is performed.

b. Both external and internal audits have an important role to play independently evaluating, on a periodic basis Agent AML & CTF procedures.

c. The External Auditor shall audit annually the adequacy of Compliance, AML & CTF procedures, Compliance officer functions, controls and shall report to the Head of AML and Management.

d. The Internal Auditor of the company shall forward a report once in six months on the efficacy of the implementation of the policy, procedures and control across the organization.

External Audit: means testing of the internal procedures by an independent party i.e., performed by people not from within the Agent. The auditors must be sufficiently qualified to ensure that findings and conclusions are reliable.

a. The independent testing by an external audit firm shall be on an annual basis.

Internal Audit: these audits may be performed internally within an organization if there is a provision of an internal audit department.

a. There should be a well-defined audit program & checklist.

b. The frequency of such audits may be once in 6 months

c. The auditor should report directly to the board of directors or to a designated board committee.

AML Compliance audit may cover the following aspects:

a. Examine the adequacy of CDD policies, procedures and processes, and whether they comply with internal requirements.

b. Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers and geographic locations) on sample testing basis

c. Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.

d. Assess compliance with applicable laws and regulations.

e. Examine the integrity and accuracy of management information systems used in the AML compliance program if any.

f. Reviewing policies, procedures, and processes for suspicious activity monitoring.

g. Determining the system effectiveness for reports, blacklist screening, flagging of unusual transactions and more.

h. Review Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transactions. Testing should include a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines (e.g., legal, private agents and banking, foreign correspondent banking) to the personnel or department responsible for evaluating unusual activity.

i. Assess the adequacy of recordkeeping.

Chapter: 7
TRAINING AND AWARENESS PROGRAM OF EMPLOYEE

7.1 Training and Awareness Program

Agent shall provide periodical Anti-Money Laundering and Counter Terrorist Financing training to all their staffs. Staffs shall be made aware of their own personal legal obligations and responsibilities under the regulations.

7.2 The Need of Awareness

a. The effectiveness of this Policy depends on the extent to which the staffs/ agents appreciate the serious nature of the background against which the legislation has been enacted.

b. In this context, Esewa Money Transfer shall introduce comprehensive measures to ensure that staffs/agents at all levels are -

- Fully aware of its internal AML/CFT measures and procedures;
- Aware that they may be held personally liable for any failure to observe the AML/CFT measures; and
- Always updated with the information on its internal AML/CFT measures and the relevant guidelines on AML/CFT issued by Nepal Rastra Bank.

7.3 Training and Awareness Program Contents

a. All relevant staff as well as agents of the company should be trained covering the following to avoid the fraud as well as to identify significant or abnormal transactions or pattern of activity. Background to money laundering and all aspects of money laundering legislation.

- The company's Customer Due Diligence (CDD) or Know Your Customer (KYC) procedures.
- The company's record maintenance procedures.
- The company's transaction monitoring procedures.
- The importance placed on the reporting of suspicious transactions, that there is a legal requirement to report, and that there is a personal statutory obligation to do so.
- Criteria that may give rise to suspicions of money laundering or terrorist financing during the course of duty
- Internal reporting line and procedures to be adopted when a transaction is deemed to be suspicions.
- Customers who avoid identifying themselves while attempting to process transactions or even providing incorrect or incomplete information.

- The customer tries to influence the staff/agents/employee not to inform the authorities about a transaction being processes of unusual nature.
- The customers refrain from providing information about their previous and current commercial activities and banking relationships and transactions
- Frequent cash deposit and withdraw by the customers without any clear reasons.
- The customer's intentional misinterpretation of information while sending/receiving amount.

Chapter: 8
AML/COMPLIANCE OFFICER (CO) DETAILS

COMPLIANCE/AML OFFICER'S DETAIL	
Name:	Rakshya Giri
Position:	Compliance Head
ID Type:	Citizenship
ID Number:	**421062-9-60**
Permanent Address:	Putali Bazzar-14, Syangja, Nepal
Current Address:	Pulchwok, Lalitpur-3, Nepal
Contact:	+977 1 5970377
Mobile:	+977 9801880274
Email:	compliance@esewaremit.com
Signature:	
Stamp:	
Date:	November 22, 2022

Annexure-A

Examples of Transactions that May Trigger Suspicion

1. Customer is evasive or unwilling to provide information when requested, especially customer who is exchanging currency equivalent to NRs. 300,000/- and above.

2. Transactions conducted are out of character with the usual conduct or profile of customers carrying out such transactions.

3. Customer using different identifications each time when conducting a transaction.

4. A group of customers trying to break up a large cash transaction into multiple small transactions.

5. The same customer conducting a few small transactions in a day or at different branches/locations.

6. There are sudden or inconsistent changes in remittance/wire transfer sent/received transactions.

7. Remittances/wire transfers from different customers/jurisdiction being sent to the same customer.

Annexure-B

SUSPICIOUS TRANSACTION REPORT

Reference No:

Internal Record form of STR Submission

S.N.	Name and address of the person	TXN No	Receiving Branch	Date of TXN	Nature of TXN	Amount	Reason to be suspicion	Remarks	Signature

Signature:

(Compliance Officer or authorized officer)

Name:

Designation:

Phone:

Email:

Date:

Annexure-C

Anti-Money Laundering & Anti-Terrorist Financing
Questionnaire for Correspondent Relationship

A. BUSINESS INFORMATION: **Date:**

1	Full Legal Name of Entity	
2	Trading Name (if different from above)	
3	Registered Full Address	
4	Primary Business Address (if different to above)	
5	Telephone Number	
6	Email ID	
7	Website	
8	Compliance Officer Name	
9	Compliance officer Contact Number	
10	Email ID	

B. LEGAL INFORMATION:

1	Type of Entity	Bank ☐	MSB ☐	MTO ☐
Private Limited ☐	Partnership ☐	Others (Please Specify):		
2	Principal Business Activity			
3	Registration Number		Reg. Date:	
4	Name of Governing/ Regulatory Authority			
5	Business/ Remittance License Number			
5.1	Issued Date:	Expiry Date:		

6	Is your company listed in any Stock Exchange? If so, Which Stock Exchange:	Yes ☐	No ☐

C. OWNERSHIP AND MANAGEMENT INFORMATION:

a. Please provide details of all shareholders owning 10% or more shares of the company.

Full Name	Shares (%)	Nationality	Date of Birth	ID/Passport Number

b. Please provide the details of Board of Directors/Senior Management list.

Full Name	Designation	Nationality	Date of Birth	ID/Passport Number

D. General AML & CFT Policies, Practices and Procedures		Yes	No
1.	Does your institution have policies and procedures approved by your institution's board or senior management to prevent money laundering and combating terrorist financing?	☐	☐
2.	Does your institution have a legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML/CFT framework?	☐	☐
3.	Has your institution developed written policies documenting the processes to prevent, detect and report suspicious transactions?	☐	☐
4.	Does your institution have a policy prohibiting accounts/relationships with shell banks*? (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.)*	☐	☐
5.	Does your institution prohibit the opening of anonymous or numbered Accounts by customers?	☐	☐

6.	Does your institution have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products?	☐	☐
7.	Does your institution have policies covering relationships with Politically Exposed Persons (PEP's), their family and close associates?	☐	☐
8.	Does your institution have policies and procedures that require keeping all the records related to customer identification and their transactions? If ''Yes'', for how long?————————	☐	☐
E.	**Risk Assessment**	**Yes**	**No**
1.	Does your institution have a risk-based assessment of its customer base and their transactions?	☐	☐
2.	Does your institution determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that have reason(s) to pose a heightened risk of illicit activities at or through the FI?	☐	☐
F.	**Know Your Customer, Due Diligence and Enhanced Due Diligence**	**Yes**	**No**
1.	Has your institution implemented processes for the identification of Beneficial Ownership *(those customers on whose behalf it maintains or operates accounts or conducts transactions)?*	☐	☐
2.	Does your institution have a requirement to collect information regarding its customer's business activities?	☐	☐
3.	Does your institution have a process to review and, where appropriate, Update customer information relating to high risk client information?	☐	☐
4.	Does your institution have procedures to establish a record for each new customer noting their respective identification documents and 'Know Your Customer' information?	☐	☐
5.	Does your institution complete a risk-based assessment to understand the normal and expected transactions of its customers?	☐	☐
G.	**Reportable Transactions for Prevention and Detection of ML/TF**	**Yes**	**No**
1.	Does your institution have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?	☐	☐
2.	Where cash transaction reporting is mandatory, does your institution have procedures to identify transactions structured to avoid such obligations?	☐	☐
3.	Does your institution screen customers and transactions against lists of person, entities or countries issued by government/ competent authorities?	☐	☐
4.	Does your institution have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin?	☐	☐
H.	**AML Training**	**Yes**	**No**
1.	Does your institution provide AML & CFT training to relevant employees of your organization?	☐	☐

2.	Does your institution communicate new AML & CFT related laws or changes to existing AML/CFT related policies or practices to relevant employees?	☐	☐
3.	Does your institution provide AML & CFT training to relevant third parties if they are employed to carry out some of the functions of your organization?	☐	☐

Space for additional information:

(Please indicate which question the information is referring to.)

Do the responses provided in above Declaration apply to the following entities of your Company? Please indicate "Yes" or "No" to satisfy.

- Head Office and all domestic branches
- Overseas branches
- Domestic subsidiaries
- Overseas subsidiaries

If the response to any of the above is ''No'', please provide a list of the branches and/or subsidiaries that are excluded, including the name of the institution, location and contact details.

I, the undersigned, confirm to the best of my knowledge that the information provided in this questionnaire is current, accurate and representative of the anti-money laundering and anti-terrorist financing policies and procedures that are established in my institution.

I also confirm that I am authorized to complete this questionnaire on behalf of my institution.

Name:	
Title:	
Contact No.:	
Email ID:	
Date:	
Signature:	

Abbreviation: NBFI*:- Non-Bank Financial Institution.

Company Seal

Annexure-D

CUSTOMER INFORMATION FORM (KYC PURPOSE)

FOR AGENT USE	
Date:	
Esewa Control No.:	
Country of Origin:	**Expected Amount:**

AGENT'S INFORMATION	
Agent Name:	
Address:	**Contact:**

SENDER'S INFORMATION	
Full name:	
Address:	
Contact No:	**Occupation:**
Type of ID: ☐ **Citizenship** ☐ **Passport** ☐ **Driving License** ☐ **Voters ID**	
☐ **National ID** ☐ **Government Issued valid ID (with photo)**	
Identity Card No:	**Issuing District:**
Issue Date:	**Expire Date:**
Nationality:	**Relationship to Beneficiary:**
Source of Fund:	**Purpose of Remittance:**

BENEFICIARY'S INFORMATION	
Full name:	
Address:	**Contact No.:**
Nationality:	**Occupation:**
Type of ID: ☐ **Citizenship** ☐ **Passport** ☐ **Driving License** ☐ **Voters ID**	
☐ **National ID** ☐ **Government Issued valid ID (with photo)**	
Identity Card No:	**Issuing District:**
Issue Date:	**Notes (If any)**
Expire Date:	
Relationship with sender:	
Purpose of Remittance:	

The information mentioned above has been matched with the original documents and nothing has been concealed. We opine the transaction has not intended for any kinds of money laundering and terrorist activities.

Customer signature

Verified By

Contact Details:

Esewa Money Transfer Pvt. Ltd.

Pulchowk, Lalitpur-3, Bagmati, Nepal

Tel.: +977 1 5970377

Toll Free: 1660-01-37777

Email ID: compliance@esewaremit.com

info@esewaremit.com

Website: www.esewaremit.com