ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

Procedural Guidelines for Defending Financial Integrity and Security

National Trust for Nature Conservation

Khumaltar, Lalitpur

2024

The 71st Governing Board of Trustees ("Board") of the National Trust for Nature Conservation ("Trust") has adopted the ***"Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Procedural Guidelines, 2024"****. These guidelines are established to provide comprehensive measures for preventing, detecting, and reporting money laundering and terrorist financing (ML/TF) activities, ensuring the highest standards of financial integrity and compliance across all operations of the Trust. The Procedural Guidelines apply to all employees of the Trust as well as to all projects and programs managed and implemented under NTNC. The Procedural Guidelines align with the Money Laundering Prevention Act, 2008, NTNC Act, 1982, NTNC Regulation, 1984, and NTNC Bye-laws, 1996. It shall come into force from the date of approval by the meeting of the Board.*

Table of Contents

SECTION – 1: INTRODUCTION

a) Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Procedural Guidelines ("Procedural Guidelines") of the National Trust for Nature Conservation (the Trust) have been developed in accordance with the Money Laundering Prevention Act, 2008 (2063) and Asset (Money) Laundering Prevention Rules, 2009 (2066) issued by the Government of Nepal.

b) The purpose of these Procedural Guidelines is to ensure compliance by the Trust, outlining its obligations and responsibilities in implementing AML/CFT measures to prevent, detect, deter and control money laundering/terrorism financing activities under the Money Laundering Prevention Act, 2008 (MLPA).

c) The Member-Secretary of the Trust holds ultimate responsibility for ensuring the Trust's compliance with the provisions of the MLPA. An internal compliance function shall be established to monitor compliance, with the Compliance Focal Person authenticating the proper role in safeguarding the Trust against money laundering and terrorist financing (ML/TF).

d) The policy shall undergo regular review and updates as necessary to reflect changes in legal/regulatory requirements or business/operational practices, including amendments to laws pertaining to AML/CFT.

1.1. What is Money Laundering?

Money Laundering is the illegal process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking or non-banking/ commercial transactions. It is the process of making illegally gained unsourced 'dirty' money into so-called sourced 'clean' money, designed to hide the source, destination, ownership, or control of funds that are intended to be used for illegal activity.

Money Laundering (ML) refers to any of the following acts:

a) The conversion or transfer of funds, by any person who knows or should have known or there are sufficient grounds for suspecting that such funds are the proceeds of illegal sources, to conceal or disguise the illicit origin of such funds or for assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his/her actions.

b) The concealment or disguising of the true nature, source, location, disposition, movement or ownership of or rights with respect to funds by any person who knows or should have known or suspects that such funds are the proceeds of crime.
c) The possession, acquisition or use of funds by any person who knows, should have known or there are sufficient grounds for suspecting that that such funds are the proceeds of crime.

1.2. What is Terrorist Financing?

Terrorism Financing (TF) refers to "An act committed by any person who in any manner directly or indirectly and willingly, provides or collects funds, support, or attempts to do so to use them by knowing that these funds may be used in whole or in part for the execution of a terrorist act or by a terrorist or terrorist organization."

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

a) Terrorism, piracy and kidnapping,
b) Drugs,
c) Illicit dealing in firearms 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.

1.3. Provisions Relating to Offences under Money Laundering Prevention Act, 2008

a) **Asset/Money not to Be Laundered:** No person shall launder or cause to launder assets.
b) **Offence of Money Laundering:** For the purpose of the MLPA, one shall be deemed to have laundered asset, in case one or any third person acquires, holds, possesses, uses, consumes, utilizes or earns or displays or transacts or deals with or causes to do so, in any manner, the asset obtained, held, possessed, directly or indirectly from commission of any or all of the following offence or act or the asset increased from

any type of investment of such asset; or converts or disguises or transfers such asset or causes to do so with an intention to conceal, convert or disguise the source, nature, place, ownership, right, disposal of such assets; or obtains, purchases, holds, possesses, uses, consumes or utilizes such asset or causes to do so; or does or causes to do transaction in any form in spite of the knowledge of such asset or with the reasonable ground to believe so; or does or causes to do any kinds of assistance directly or indirectly to transform, change or transfer such asset or causes to do so.

- Revenue evasion,
- Organized crime,
- Financing of terrorist activities,
- Offence under existing law on arms and ammunition,
- Offence under existing law on foreign exchange regulation,
- Offence under existing law against homicide, theft, fraud, forging of documents, counterfeiting, abduction or hostage taking,
- Offence under existing law on narcotic drug control,
- Offence under existing law on national park and wildlife conservation,
- Offence under existing law against human trafficking and transportation,
- Offence under existing law on cooperative institutions,
- Offence under existing law on the forest,
- Offence under existing law against corruption,
- Offence under existing law on bank and financial institutions,
- Offence under existing law on banking offences and penalty,
- Offence under existing law on ancient monument conservation,
- Offence on smuggling (paying without customs duty, excise and other tax),
- Offence on extortion and piracy,

- Offence under any other law or treaty to which Nepal is a party, as designated by the Government of Nepal through publishing a notice in Nepal Gazette.

c) **Prohibition on Financing of Terrorist Activities:** No one shall finance or cause to finance terrorist activities.

d) **Offence of Financing of Terrorist Activities:** Any person commits the offence of financing of terrorist activities if that person by any means collects or provides to any person any asset with the intention that they should be used or in the knowledge that they are to be used in order to carry out any act which constitutes an offence within the scope of the following conventions or any other act intended to cause death or serious bodily injuries to an individual.

- Tokyo Convention on Offences and Certain Other Acts Committed on Board Aircraft, 1963,
- Hague Convention for the Suppression of Unlawful Seizure of Aircraft, 1970,
- Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 1971,
- Convention on the Prevention and Punishment of Crime Against Internationally Protected Persons Including Diplomatic Agents, 1973,
- International Convention Against the Taking of Hostages, 1979,
- SAARC Regional Convention on Suppression of Terrorism, 1987,
- Any Convention against Terrorist Activities to which Nepal is a party.

e) **Not to Attempt, Abet or Provoke:** No one shall attempt, abet or incite others to commit offences stipulated in this chapter.

f) **Penalty for the offence committed abroad:** Notwithstanding anything contained in the MLPA, any act or offence mentioned in Section 3, 4, 4A, 4B of the MLPA committed abroad shall be dealt as an offence and may be liable to a penalty as if they were committed in Nepal, provided that the act or offence is punishable offences in

the foreign country where such offences were committed and such country has not imposed the penalty for the offence.

1.4. Different Stages Involved in Money Laundering

Money laundering typically involves three stages, which may occur separately, simultaneously, or in overlapping phases. In each stage, illegally obtained money is introduced and integrate into the financial system through financial institutions.

a) Placement

The first stage of money laundering involves introducing illegally obtained funds into the financial system. Generally, this is done by breaking up large amounts of cash into smaller sums to deposit directly into a bank account or by purchasing monetary instruments or stocks. Techniques such as false invoicing, smurfing (depositing cash below the AML reporting threshold frequently), and hiding beneficial owners, are commonly used. Placement integrates physical cash obtained from illegal activities into the financial system, enhancing the liquidity and accessibility of the funds. Money launderers employ various techniques during this stage, such as depositing cash into bank accounts, purchasing insurance products, and using cash to acquire assets.

b) Layering

The layering stage is when the launderer moves the illegal money through a series of financial transactions to make it difficult to locate the source. To obscure the illegal origin of the placed funds and increase their usability, money undergoes a layering process involving movement, dispersal, and disguise. At this stage, money launderers use techniques like multiple bank transactions, engaging intermediaries such as professionals, and conducting transactions through corporations and trusts. These methods create complex layers of financial transactions designed to obscure the audit trail and provide anonymity. The primary objective of layering is to dissociate illegal funds from their source, effectively concealing their origin and ownership through a sophisticated network of financial activities. Specifically, the accounts of money launderers are often scattered and are most likely to be found in tax haven jurisdictions.

c) Integration:

The integration stage of money laundering is the final step in the money laundering process. In this stage, the launderer attempts to integrate illicitly obtained funds into the legitimate financial system. These funds are used to buy goods and services, real estate, luxury assets, houses cars and other items without attracting attention from law enforcement agencies in related jurisdictions. The “cleaned” funds can now be made available for investment in legitimate or illegitimate businesses. As a result, the originally "dirty" money appears legitimate. By this stage, distinguishing between legal and illegal wealth becomes exceedingly challenging.

1.5. Punishment to the Offender of Money Laundering

According to Sub-Section 30 of the MLPA, individuals committing offenses under Section 3 shall be subject to the following punishment penalties, depending on the severity of the offense:

i. Any person who commits the offense of money laundering set forth in sub-section (1) of Section 3 shall be liable to a fine of twice the claimed amount and imprisonment for a term of two to fifteen years, depending on the gravity of the offense.
ii. Any person who conspires to commit the offense of money laundering, as set forth in sub-section (2) of Section 3, shall be liable to the same sentence as in sub-section (1). Any person who commits any other related offenses shall be liable to half the sentence set forth in sub-section (1).
iii. Any person who commits the offense of terrorist financing as set forth in sub-section (1) of Section 4 shall be liable to a fine of five times the claimed amount, or up to fifty million rupees if the claimed amount is not specified, and imprisonment for a term of seven to twenty years, depending on the gravity of the offense.
iv. Any person who commits the offense of terrorist financing as set forth in sub-sections (2), (3), or (4) of Section 4 shall be liable to half the sentence specified in sub-section (3).
v. If any person commits an offense of money laundering or terrorist financing using a legal person or legal arrangement, the person, office-bearer, or employee responsible shall be liable to the sentences specified in sub-sections (1), (2), (3), or (4).
vi. If the person, office-bearer or employee referred to in sub-section (5) cannot be identified, the person who acted as the chief at the time of commission of the offence shall be liable to action pursuant to the prevailing laws.

vii. If any public servant or office-bearer or employee of a reporting entity commits any offence of money laundering or terrorist financing, such person shall be liable to an additional ten percent of the sentence, in addition to the sentence set forth in sub-section (1), (2), (3) or (4).

vii A. A person who has an obligation to prevent an offense under this Act, may be imprisoned for one year if he/she allows an offense to be committed while having reasonable grounds to know that an offense may be committed or is going to be committed without fulfilling his/her responsibility to prevent such an offense from occurring.

viii. If any legal person commits any offence of money laundering or terrorist financing, such legal person or legal arrangement shall, notwithstanding anything contained in the prevailing laws, be liable to any or all of the following sentences, depending on the gravity of offence:

(a) imposing a fine up to five times of the fine imposable under sub-section (1), (2), (3) or (4),

(b) prohibiting from participating in public procurement for a certain period to be specified,

(c) prohibiting from procuring goods or services for a certain period to be specified,

(d) getting recovered damages for loss and damage,

(e) revoking the license or permit, or

(f) dissolving such legal person.

ix. Any person who violates this Act or the rules framed under this Act, except that set forth in sub-sections (1) to (8), shall be punished with the sentence of a fine equal to the claimed amount, along with confiscation of the claimed amount, if set out, and a fine not exceeding one million rupees if the claimed amount is not set out.

x. If the beneficial owner is found to be involved in the offense mentioned in this Act, he/she shall also be liable to punishment according to this Section.

a) Liable to imprisonment from two year to five fifteen years and a fine equivalent to the claimant value where claimant value is identified and up to five hundred thousand rupees where the claimant value is not identified.

b) Other than one mentioned above shall be liable to a fine equivalent to the claimant value and one year to four years of imprisonment.

c) If any bank, financial institution, or non-financial institution has committed an offense, the official or staff of such institution identified as the perpetrator of the offense, or if such perpetrator is not identified, the official acting as the chief of the institution at the time of the offense, shall be liable to penalty.

d) If any civil servant, official, chief, or staff of any bank, financial institution, or non-financial institution has committed the offense, such person shall be liable to an additional ten percent punishment on top of the punishment mentioned in Sub-sections (1) and (2) of the MLPA.

e) Anyone who attempts, assists, or incites the offence under the MLPA shall be liable to half of the punishment awarded for the commission of the offence.

f) If anyone commits or cause to commit offence under the MLPA by using any firm, company or institution, such firm, company or institution shall be liable to the fine mentioned in this section.

g) If anyone violates the MLPA or the rules or directives under this Act in a manner other than those provided for in Sub-section (1) to (6), one shall be liable to a fine equivalent to claimant value by confiscating such value and up to five hundred thousand rupees where such value is not identified.

1.6. Implementation of the AML/CFT Measures

In carrying out fund transfer activities, the Trust shall establish and implement effective AML/CFT measures in order to mitigate the possible risk of money laundering, terrorist financing and other illegal fund transactions. These AML/CFT measures include the following:

a) **Due Diligence:** Conducting due diligence to identify and verify information pertinent to transactions such as grants, subsidies, donations and investments;

b) **Record Keeping:** Maintaining comprehensive records and documentation related to transactions conducted by the Trust;

c) **Ongoing Transaction Monitoring:** Continuously monitoring transactions to ensure that maintained information remains current and relevant, facilitating the detection of suspicious activities;

d) **Suspicious Transaction Reporting (STR):** Submitting reports on suspicious transactions to the designated government agency when the Trust suspects involvement in money laundering, terrorism financing, or other unlawful activities.

e) **Legal Person and Legal Arrangement:** Ensuring the legitimacy of funds received from any fund manager, charity organization, development fund, company, corporation, partnership firm, cooperative, or other similar entity or legal arrangement.

f) **Risk-based Approach:** Adopting a management approach to identify and address the potential risks of ML/TF while obtaining funds.

g) **Informing Government Agencies:** Informing concerned government agencies about potential risks of ML/TF as the informer organization.

h) **Assessing Compliance:** Assessing the compliance of AML/CFT regimes by partner organizations or firms associated with the implementation of programs financed by the Trust.

SECTION – 2: AML/CFT INSTITUTIONAL FRAMEWORK

2.1. General Guidelines

The Trust is committed to fulfilling its AML/CFT obligations to actively prevent transactions that could facilitate money laundering, criminal activities or terrorism. To achieve this, the Trust has formulated and implemented this procedural guideline for internal controls, aiming to prevent criminals from exploiting its facilities for ML/TF. This ensures compliance with legal requirements.

The internal control measures encompass:

- Conduct regular assessments to identify and mitigate risks associated with ML/TF;
- Develop guidelines that address timing, control levels, areas of oversight, responsibilities, and follow-up actions to combat ML/TF;
- Monitor unusually large and suspicious transactions and apply enhanced due diligence to individuals and businesses posing high risks, including politically exposed persons (PEPs);
- Provide information associated with ML/TF suspicious funds transactions to financial institutions and law enforcement agencies;
- Implement enhanced due diligence measures and mechanisms for individuals in jurisdictions lacking adequate AML/CFT regulations;
- Provide comprehensive training to employees, including the Compliance Focal Person, on due diligence practices and the identification and handling of suspicious transactions; and
- Ensure employees are well-informed about AML/CFT laws, regulations, and procedural guidelines established by the Trust in accordance with these laws.

2.2. Appointment of Compliance Focal Person

The Trust shall appoint a responsible official as a Compliance Focal Person equipped with the relevant competence, authority and independence to implement the Trust's AML/CFT compliance.

2.3. Co-operation with Competent Authorities for Information

The Trust shall comply promptly with requests, and pursuant to the law, provide information to the competent authority or other relevant government agency, including searching records for accounts or transactions related to the individuals or entities named, reporting the findings, and ensuring the confidentiality and security of the requests.

SECTION – 3: DUE DILIGENCE

3.1. Risk Assessment of the Trust's Activities

Internationally, instances abound where funding institutions and charities have been exploited by terrorist organizations to provide financial and logistical support for their operations. Therefore, the Trust must be vigilant regarding its activities and financial transactions, especially in countries prone to ML/TF activities, as cross-border fund flows may elevate the risk of terrorist financing or money laundering. Understanding these risks not only helps the Trust take proactive steps to mitigate them and prevent misuse by criminals and terrorists but also explains why financial institutions may view the sector as high-risk for ML/TF.

Given the higher risks associated with receiving and disbursing financial support, charity as well as investment and support, the Trust shall undertake thorough due diligence in accordance with this policy when assessing donors, beneficiaries, and partner organizations.

3.2. Due Diligence

a) Due Diligence: is about knowing, identifying and evaluating the counterparty, who the Trust is dealing with, be it an existing or a new.

b) Effective due diligence enables the Trust to identify potential transactions related to money laundering, terrorist financing, or other illegal activities at the point of contact with counterparties, thereby safeguarding against financial crimes and unlawful activities.

c) Enhanced Due Diligence involves gathering additional information, including but not limited to:

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

- Delivery channel,
- Remitters business and source of funding.

3.3. Requirements under Due Diligence

a) Donor Due Diligence

i The donor due diligence exercise involves screening potential donors to assess whether they pose a significant risk of ML/TF. This process includes identifying the donor, verifying their identity, and conducting high-level media screening. It also allows the Trust to ensure that the donor's profile aligns with the Trust's purpose and objectives. The process should be risk-based, meaning that higher-risk donors require more extensive due diligence. This approach ensures that disproportionate time is not spent on reviewing low-value/low-risk donations.

ii The enhanced due diligence shall be conducted for jurisdictions and individuals receiving funds as the grey list designated by FATF (Financial Action Task Force), Financial Intelligence Unit (FIU), and Ministry of Home Affairs, Government of Nepal.

iii The Trust shall conduct due diligence in line with the following guidelines, bearing in mind that the application of a risk-based approach may require flexibility in case of individual and the globally reputed funds, created on the basis of the agreement under the UN system and others. The thresholds shall depend on the Trust's risk profile, risk appetite, donor profiles, and resource constraints.

A. Standard due diligence:

i Domestic donations with no Higher Risk Factors and/or other reasons for suspicion;

ii Donations with an international element with no Higher Risk Factors and/or other reasons for suspicion;

iii Donations with a single Higher Risk Factor (other than sanctions or PEP) risk.

B. Enhanced due diligence:

i Donations as decided by senior management team;

ii Donations with potential sanctions or PEP (Domestic and Foreign) risk;

iii Donations with multiple higher risk factors or those that are otherwise atypical, unusual, or suspicious based on the Trust's experience; and/or

iv Donations from donors domiciled in high-risk countries as recommended by the FATF and informed by the national FIU and the Ministry of Home Affairs.

C. Summary table:

Nature of donation	**Monetary Threshold over which Due Diligence should be completed**	**Type of Due Diligence**
Domestic only – e.g. originates from the resident country and shall be used to benefit the country's beneficiaries/society + no Higher Risk Factor	Per senior management team decision	Standard
International – e.g. originates from a donor outside of the country and/or is intended benefit beneficiaries/communities outside of country + no Higher Risk Factor	Per senior management team decision	Standard
Domestic or international donation with one Higher Risk Factor (other than potential sanctions risk for which see below)	Per senior management team decision	Standard
Multiple Higher Risk Factors and/or potential sanctions or PEP issue	Any	Enhanced
High value donation + no Higher Risk Factor	Per senior management team decision	Enhanced

v The Trust shall not as a matter of usual practice undertake due diligence on donations below the threshold set out by the senior management team decision given the generally low risk of such smaller donations, as well as the impracticality of identifying the identity of small donors (e.g., street collections, charity boxes).

- No anonymous donations shall be accepted (without the approval of the Board).

vi The due diligence process shall be undertaken prior to or otherwise as soon as possible on acceptance of a donation from a new donor.

vii Standard Due Diligence

- Step 1: Identification and verification
- Step 2: Name screening

- Step 3: Country's Risk profiling as listed by FATF

viii Enhanced Due Diligence for Higher Risk Situations

- No donations should be accepted by the Trust where material high-risk factors are present and cannot be mitigated. The approval of the Member Secretary should be obtained to commence or continue any such relationship.

ix Ongoing monitoring

- The Trust shall ensure that the due diligence on its donors is regularly reviewed and kept up to date. A risk-based approach should be applied in this regard, meaning that the due diligence relating to the higher risk donors should be reviewed more frequently (e.g., on a half-yearly annual basis) than that of the lower risk donors.

b) Beneficiary Due Diligence:

i. Beneficiary risk
    - To the extent that the Trust distributes cash or other forms of financial support directly to individuals or entities who meet its eligibility requirements ("Beneficiaries"), it is important that the Trust takes reasonable steps to ensure that any funds so provided are used in accordance with the Trust's objectives as set out in the Trust's act, regulations and bye-laws, and not for illicit purposes. These steps will include undertaking risk-based due diligence on the Beneficiary and conducting reasonable checks on the end-use of the donations. If financial support is provided by the Trust through a third party/partner organization, reasonable due diligence should also be carried out on that organization as well.

ii. The Trust's senior management team must ensure that the Trust's funds are used by the Beneficiaries in accordance with the Trust's objectives, approved plans, and programs. To fulfil this duty, the Trust shall conduct reasonable/periodic and proportionate follow-up monitoring on Beneficiaries after any such financial assistance is provided.

c) Partner Due Diligence

i. To the extent that the Trust works with partner organizations to further the Trust's objectives, reasonable due diligence should be carried out on those entities as appropriate so as to check that that partner is bonafide, not involved in any activities

related to ML/TF, and properly managed, as well as having a willingness to mitigate the risk of inadvertently working with fraudulent or otherwise criminal organizations.

ii. A risk-based approach to due diligence should also be applied when reviewing partner organizations.

iii. As part of general anti-fraud measures, the Trust should also at a minimum:

- Undertake name screening and other forms of background checks (e.g., reference checks) of all new individuals as part of the onboarding process; and
- Complete at least standard due diligence on suppliers with whom the Trust has a material (in terms of monetary value or importance to its operations) and/or continuing (i.e., not a "one-off") contract.

d) Third-Party Transactions

i. "Third-party transactions" refer to transactions where the Trust receives funds from, or is asked to remit funds to, a third party other than the donor, beneficiary or partner on whom the Trust has undertaken its due diligence. This may occur when:

- The Trust is requested by a beneficiary or partner to whom it has agreed to provide funds to instead remit those funds to a third party; or
- The Trust unexpectedly receives funds from a third-party payer/account instead of directly from the donor.

ii. The Trust should not accept or agree to third party transactions other than in exceptional circumstances where the Trust is satisfied that:

- Enhanced due diligence on the third-party payer or payee presents no material money laundering or terrorist financing risk;
- The relationship between the donor, beneficiary or partner and the third-party payer/payee is transparent, credible and documented;
- There is a legitimate, credible and documented explanation for the involvement of the third party; and
- The Member Secretary approves the third-party transaction.

iii. Based on the risk-based approach, the Trust's Compliance Focal Person should classify the risk categories as High Risk, Medium Risk, Low Risk and No Risk for all partners including donors and recipients, with the prior approval of senior management team.

iv. The Trust should maintain Customer Due Diligence (CDD), which involves identifying and verifying customers or recipients of the Trust's funds who are willing to work with or have already worked with the Trust.
v. The beneficial owner (a natural person who ultimately owns or controls the account of another person for money laundering purposes or to evade charges for any predicate offense) should be identified for receiving and disbursing funds.
vi. If the Trust cannot satisfy itself that the third-party transaction is acceptable following the steps described above, the Trust must decline the transaction and consider its reporting obligations.

SECTION – 4: RECORD KEEPING REQUIREMENTS

4.1. Record Keeping

a) An efficient records management program is essential and must proactively and effectively manage all data, media, and information. Policies and procedures that set standards demonstrate management's support and investment in a complaint records management program. These procedures should be clearly communicated and easily accessible. Consistent record retention practices shall be implemented across the Trust. When properly employed, these practices should integrate seamlessly with the Trust's other relevant plans and programs.

b) The Trust should retain either the original or a scanned/photocopied copy of documents used to identify and verify counterparties/ donors/ partners/ beneficiaries. In addition, the Trust shall keep records of all other relevant information (e.g., results of name screening) including Suspicious Transaction Report (STR) and Threshold Transaction Report (TTR) and Beneficial Owner obtained during the due diligence process as outlined in this Procedural Guidelines. These records should be maintained for all counterparties, including donors, partners, beneficiaries, individuals acting on their behalf, other connected parties, and/or any organizations with whom the Trust establishes a working relationship.

4.2. Document retention

a) In general, the Trust shall retain all records obtained through due diligence measures, documentation regarding counterparty relations and executed transactions, and correspondence with the counterparties for a minimum period of five (5) years. Additionally, all such documents and records should be retained throughout the duration of the relationship with the donor/partner/beneficiary. After the termination of the relationship, the records shall be kept for a period determined by the senior management team.

b) Records must be maintained in a format that enables the creation of an audit trail for individual transactions, ensuring they are traceable by relevant financial institutions law enforcement agencies.

c) Records can be retained in paper or electronic form.

SECTION – 5: TRANSACTION MONITORING AND CONFIDENTIALITY

5.1. Recognition and Reporting of Suspicious Transactions

There is no precise regulatory definition of what constitutes suspicious activity, but a suspicious transaction typically deviates from the counterparty's known legitimate business or personal activities, or from the normal operations expected for that type of account. Transactions involving large amounts of cash or conducted repeatedly and unnaturally may indicate suspicious activity. Suspicious activity can occur during initial negotiations with a prospective counterparty to establish a collaborative relationship, at the commencement of the counterparty relationship, or even long after the relationship has begun.

5.2. Obligation for Reporting of Suspicious Transactions

The Trust is obligated to submit a Suspicious Transaction Report (STR) to the government regulatory body, following due official processes, whenever any of its employees/counterparty (ies) suspect or have reason to suspect that a transaction involves proceeds from unlawful activity, or that the counterparty is engaged in money laundering or terrorism financing.

5.3. Mechanism for Reporting of Suspicious Transactions

a) The Trust's responsible officials must remain vigilant for transactions that are inconsistent with the counterparty's due diligence information.
b) If any unusual transaction is identified, the employee observing it shall promptly complete the "Suspicious Transaction Report (STR) Form" and submit it to the Compliance Focal Person. This form has to be developed by the Compliance Focal Person consulted with the regulatory authority and approved by the Member Secretary upon senior management team decision.
c) The Compliance Focal Person shall thoroughly evaluate the reported incident in light of all relevant information, documenting in writing with detailed reasons whether the transaction is linked to money laundering or terrorist financing.
d) If the reported issue does not appear to involve money laundering or terrorist financing, the Compliance Focal Person shall close the matter after recording comments on the STR form.
e) If the reported issue appears to involve money laundering or terrorist financing, the Compliance Focal Person shall submit the STR to the concerned regulatory authority through appropriate channels such as email or fax.

f) The Compliance Focal Person is granted the necessary independence to report suspicious transactions following due official processes, without requiring approval from the senior management team for this purpose.

g) Additionally, the Compliance Focal Person is authorized to collaborate with government authorities, including providing additional information and documents, and promptly responding to any further inquiries related to the STR.

h) STR Register: All investigative matters must be documented in a register. The register should include details of the investigation issue and rationale for case disposition. Furthermore, any unusual activities for which a decision was made not to file an STR should also be recorded in the register.

5.4. Red Flags – Possible Suspicious Fraud Activity Signals

a) A transaction may exhibit certain 'red flags' that raise suspicion of its connection to criminal activity or criminals. These 'red flag' features are described as indicators in accordance with the Guidelines for Suspicious Transactions Reporting (STR) developed by Nepal Rastra Bank. It is crucial that Trust employees, more particularly the Compliance Focal Person, can identify these indicators, especially those relevant to their specific business, to determine if a transaction is suspicious. The presence of one or more indicators may not constitute evidence of criminal activity; however, it can raise suspicion. The presence of multiple indicators should signal that additional inquiries may be necessary. Additional inquiries conducted by the Compliance Focal Person can help either dismiss or substantiate the suspicion.

b) Various indicators exist for detecting suspicious transactions. To expedite the detection of STRs and prevent money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction, these indicators have been categorized into: 1) General and 2) Sector-specific indicators. These indicators serve as a guide and are not exhaustive lists of all possible indicators. The Trust's employee shall be aware that criminals and organized crime groups regularly adapt their behaviour to exploit weaknesses across different industries for laundering funds.

5.5. Ongoing Monitoring of Transactions

c) The Trust shall conduct ongoing monitoring of its transactions and regular counterparty(ies) to ensure that maintained records/information are up-to-date, facilitating the detection of any suspicious transactions that may appear inconsistent with expected patterns of counterparty(ies).

d) Due to the diverse types of transactions potentially used by money launderers or terrorist financiers, defining a suspicious transaction can be challenging. Generally, a suspicious transaction is one that deviates from a counterparty's known legitimate business or personal activities.

e) While reporting suspicious transactions to the relevant government authority, the Trust shall follow the provisions specified by the MLPA. This includes considering transactions that are suspicious due to their potential link to criminal activities, terrorism, or related activities. The Trust shall report all suspicious transactions, including attempted transactions, regardless of the transaction amount.

f) Various indicators exist for detecting suspicious transactions. The Trust shall install or develop and implement, as well as maintain a standardized system to identify such transactions.

g) Transactions meeting the criteria for suspicious transactions shall undergo heightened scrutiny by the Compliance Focal Person. The Compliance Focal Person shall assess whether a STR should be submitted to the relevant government authority.

h) The trust must report transactions beyond the prescribed threshold limits to the regulatory authority (TTR)

5.6. Maintain Confidentiality and Secrecy

Trust officials must exercise caution when dealing with counterparty (ies), ensuring their actions do not cause undue alarm or disclose information to unauthorized individuals. At no level shall any official divulge information regarding reported unusual or suspicious transactions or any other details to counterparties or any other person. Such disclosures could potentially hinder or adversely influence the investigation process. This Procedural Guidelines applies except where permitted under the provision of MLPA.

5.7. Blacklisted Entities and Individuals

a) The Compliance Focal Person shall continually, and on an as-needed basis, obtain information on blacklisted entities and individuals from regulatory authorities and international agencies, updating this information in the system. All transactions with counterparties shall undergo a screening process using authorized sanction screening tools.

b) The blacklist scanning function shall be conducted at the Trust's Central Office. All transactions, regardless of the amount, shall be scanned against the blacklist database. If there is a name match with a counterparty beneficiary or any jurisdiction, the transaction shall be immediately suspended, and an alert shall be sent to the Finance Department. The counterparty beneficiary details of the suspended transaction shall then be verified against the blacklist, database. If the details do not match, the suspension shall be revoked. If there is an exact match, the transaction shall be blocked and reported to the regulatory authority following the official process.

c) The Compliance Focal Person shall furnish available details to the regulatory authority or any other law enforcement authorities upon request within a reasonable period of time, maintaining the due official channels.

d) In case there is any doubt that a transaction is intended for a terrorist organization or terrorist purposes, the Trust shall freeze the transaction and inform the relevant government authority in writing immediately, following the due official process.

5.8. Politically Exposed Persons (PEPs)

Politically Exposed Persons (PEPs) present potentially higher risk situations, necessitating additional due diligence. PEPs are individuals entrusted with prominent public functions, their immediate family members, or persons known to be close associates of such individuals. Public functions exercised at levels lower than the national level are generally not considered prominent. However, if their political exposure is comparable to that of a similar position at the national level, they should be considered PEPs on a risk-sensitive basis.

The Trust shall maintain a list of PEPs receiving data from Government of Nepal, FIU of Nepal Rastra Bank or from related entities. Due diligence shall be conducted for all PEPs while receiving and disbursing the funds.

5.9. Procurement related AML/CFT Matters

The Trust ensures its commitment to restrict all forms of procurement free from ML/TF activities. The following provisions shall be put in place in this regard:

- All offices and departments of the Trust shall conduct due diligence to verify and identify the ML/TF acts for all forms of procurement process;
- The procurement section shall take the necessary measures to prohibit the trade-based Money laundering;
- It shall be the responsibility of procurement section to report to the Compliance Focal Person any cases of suspicious procurement attempts; and
- The Trust shall prepare the list of trade-based money laundering indicators to aid in the procurement process. This list shall be disseminated to all concerned offices and departments in writing and through training.

SECTION – 6: ROLES AND RESPONSIBILITIES

6.1. Roles and Responsibilities of the Board

The NTNC Board shall oversee the functions related to AML/CFT executed by the Member Secretary. The roles and responsibilities of the Board include:

- Discussing and reviewing reports submitted by the Member Secretary on AML/CFT;
- Providing approval to the Member Secretary for submitting STRs and TTRs to the regulatory authorities of the Government of Nepal,
- Formulating policies for identifying and verifying persons and entities at risk of ML/TF,
- Overseeing and directing management for the effective implementation of a risk-based approach, including handling PEPs and beneficial owners when receiving and disbursing funds.

6.2. Roles and Responsibilities of the Member Secretary

The specific roles and responsibilities of the Member Secretary include:

- Submitting reports on activities conducted under these guidelines to the Board.
- Directing, supervising, and continuously monitoring the activities performed by the Compliance Focal Person.
- Reviewing existing policies and guidelines for effective implementation of AML/CFT measures and reporting to the Board for discussion and approval.
- Conducting an annual AML/CFT risk assessment for the Trust.
- Providing necessary resources and authority to the Compliance Focal Person to conduct activities as prescribed in the guidelines.

6.3. Roles and Responsibility of Compliance Focal Person:

The specific roles and responsibilities of the Compliance Focal Person include:

- Accessing any records, books of accounts, and relevant documents necessary to perform the activities outlined in these guidelines without prior approval from the Board or Member Secretary.
- Implementing the required activities to enforce the guidelines effectively.
- Acting as the focal point for the effective implementation of the AML/CFT guidelines within the Trust, in coordination with government regulatory authorities.
- Monitoring the Trust's compliance status in accordance with these guidelines.

- Reporting progress, issues, and potential solutions to the Member Secretary regarding AML/CFT matters on a monthly basis.
- Developing an AML/CFT Compliance Program and submitting it to the Member Secretary for approval.
- Receiving and vetting suspicious transaction reports from employees.
- Filing suspicious transaction reports with the competent/supervisory authority.
- Timely filing of other statutory reports with the competent/supervisory authority.
- Coordinating employee training on AML/CFT awareness, detection methods, and reporting requirements.
- Serving as a liaison with relevant competent/supervisory authorities and as a point-of-contact for all employees on issues related to ML/TF.

SECTION – 7: MISCELLANEOUS

TRAINING AND AWARENESS

7.1. Employee Training

a) All employees of the Trust shall:

   i. Receive a copy of these Policy Guidelines and provide written confirmation annually that they have read and understood them; and

   ii. Complete AML/CFT training as advised by the Compliance Focal Person as soon as possible upon commencing employment with the Trust.

b) Employees shall be informed of their personal legal obligations and responsibilities under relevant regulations.

c) Employees shall be made aware of their obligations under applicable laws, including the requirement to identify and properly manage transactions or activity(ies) potentially related to ML/TF.

d) Refresher training shall be provided to employees on a regular basis, particularly for those directly engaging with counterparties, including donors/partners/beneficiaries.

e) AML/CFT training sessions shall be incorporated into all regular training programs lasting three days or more.

f) High-level general awareness training programs shall be conducted for senior management to enhance their understanding and awareness of AML/CFT issues.

g) The Trust shall conduct the knowledge-sharing programs with competent government authorities and other relevant institutions concerning AML/CFT.