ANTI-TERRORISM AND ANTI-MONEY LAUNDERING POLICY

Version	**1.1**
Reviewed	**Legal Division**
Approval Body	**Board**
Approval Date	**January 2024**
Effective Date	**January 2024**
Applicability	**LISUDEV**

1. INTRODUCTION

This policy applies to all Local Initiative for Sustainable Development (LISUDEV) staff, partners, contractors, vendors, suppliers, implementing partners, and other third parties with whom it enters into financial, contractual, or operational relationships. This policy states that LISUDEV will comply with all applicable laws and regulations to ensure that:

- LISUDEV funds or property are not used for terrorism or terrorist activities.
- LISUDEV is not used as a vehicle for money laundering; and
- LISUDEV does not engage in any financial transaction or other dealing that engages a prohibited party;

1.1, POLICY STATEMENT

LISUDEV has 'ZERO TOLERANCE FOR MONEY LAUNDERING, TERRORIST FINANCING, FRAUD, CORRUPTION, BRIBERY, AND ANY OTHER FORM OF FINANCIAL CRIME'.

a) LISUDEV will comply with all applicable laws, regulations, donor requirements, contractual obligations, and internationally recognized standards relating to Anti-Terrorism and Anti-Money Laundering (ATAML), Counter-Terrorist Financing (CTF), Anti-corruption, and financial crime prevention. This includes compliance with relevant laws of Cameroon, CEMAC regulations, and United Nations Security Council sanctions.
b) LISUDEV must not engage in, support, facilitate, or be associated with any terrorist activity, terrorist organization, or individual linked to terrorism.
c) LISUDEV will not participate in any financial transaction, transfer of resources, provision of services, procurement activity, partnership arrangement, or other dealing that directly or indirectly benefits, supports, or involves a prohibited, sanctioned, or restricted party.
d) LISUDEV must not be used as a vehicle for money laundering, terrorist financing, fraud, corruption, or any activity involving criminal property.
e) LISUDEV prohibits the acquisition, possession, concealment, transfer, conversion, or use of funds or assets derived from criminal activity and must not participate in any transaction intended to disguise the origin, ownership, location, movement, or control of criminal proceeds. None of its funds, assets, property, resources, personnel, programs, or activities should be used for terrorism, terrorist financing, or any other prohibited transaction.
f) Where any actual or suspected dealings with prohibited parties, terrorist financing, money laundering, fraud, corruption, or other financial crimes are identified, LISUDEV will take immediate and appropriate action to ensure a swift, effective, and appropriate response. Such action may include investigation, suspension of transactions, reporting to competent authorities, donor notification where required, disciplinary measures, recovery of assets, termination of partnerships, and implementation of corrective actions to prevent recurrence.
g) However, exceptional circumstances may arise where a payment is made under duress to protect against an imminent threat to the life, health, safety, or liberty of staff members or others. Any staff member who makes such a payment under these extreme circumstances must report the incident as soon as it is safe and practicable to do so. Staff acting under such duress will not be subject to disciplinary action.

1.2. PURPOSE

The purpose of this Anti-Terrorism and Anti-Money Laundering (ATAML) policy is to ensure that LISUDEV upholds the highest standards of integrity, accountability, transparency, and compliance across all its operations and financial activities. This policy and its associated procedures are designed to ensure that LISUDEV:

- LISUDEV complies with all applicable laws, regulations, donor requirements, contractual obligations, funding requirements, and international standards.

- LISUDEV conducts appropriate due diligence and risk assessments of partners, suppliers, contractors, staff, consultants, and other third parties;
- LISUDEV promotes a culture of ethical conduct, accountability, transparency, and compliance throughout the organization;
- LISUDEV ensures that resources entrusted to the organization are used solely for legitimate charitable, humanitarian, development, and organizational purposes in accordance with its mission and objectives.
- LISUDEV maintains effective systems and controls to prevent, detect, and report suspicious activities, financial crimes, and prohibited transactions; and
- Protects its assets, resources, reputation, and programs from misuse, diversion, fraud, corruption, money laundering, terrorist financing, and other financial crimes;

2. SCOPE

This policy applies to all LISUDEV's staff, Board members, and partners. LISUDEV will terminate its involvement with any individuals who fail to comply with this policy. The policy also applies to all consultants and contractors. All partners, donors, and suppliers are also subject to the measures to prevent financing terrorism and/or money laundering in compliance with the (ATAML) laws in the state of Cameroon and International Standards.

3. COMPLIANCE SCREENING AND DUE DILIGENCE

- To mitigate the risk of engaging with prohibited, sanctioned, or high-risk individuals and entities, LISUDEV must undertake due diligence and legal compliance screening for employees, consultants, contractors, vendors, suppliers, implementing partners, and other third parties with whom it enters into financial, contractual, or operational relationships using available sanctions lists, watch lists, and other publicly available compliance resources, and other recognized international compliance databases.
- Screening is conducted before establishing a financial or contractual relationship and periodically thereafter based on risk assessments.
- LISUDEV will not employ, fund, contract, engage, transfer funds to, procure from, or otherwise enter into a financial or business relationship with any individual or organization, including employees, consultants, contractors, partners, vendors, suppliers, and donors—until appropriate due diligence and compliance screening have been completed and no material compliance concerns have been identified.
- All individuals and entities subject to screening must be recorded in the applicable LISUDEV systems, including but not limited to: Human Resource records and personnel files;

Procurement and vendor management records; Partner due diligence and partnership management records; Grant and donor management records; and other official organizational databases and recordkeeping systems.

- This requirement applies to all forms of financial transactions and transfers, including cash payments, bank transfers, mobile money transactions, and electronic payments.
- LISUDEV does not conduct compliance screening of programme participants or community members receiving humanitarian, development, or social support services.

3. REPORTING OBLIGATIONS AND INCIDENT MANAGEMENT

3.1 Mandatory Reporting

All LISUDEV members, employees, consultants, volunteers, interns, contractors, and implementing partners have a duty to promptly report any suspicion, concern, allegation, or knowledge that LISUDEV, its personnel, partners, contractors, suppliers, vendors, donors, or other associated parties may have intentionally or unintentionally:

- Engaged in a prohibited transaction;
- Provided financial, material, logistical, or other support to an individual or entity associated with terrorism, terrorist financing, sanctions violations, organized crime, money laundering, corruption, fraud, or other unlawful activities;
- Report to your immediate supervisor or line manager; or use the email: reportcase@lisudevcm.org.

Personnel are encouraged to report concerns based on reasonable suspicion and should not wait until conclusive proof has been obtained before making a report. All suspected or actual incidents must be reported regardless of:

- The financial value involved;
- The perceived severity of the incident;
- Whether the matter has already been reported under another policy or procedure;
- Whether another organization or third party is conducting an investigation; or
- Whether complete evidence is available.

3.2 Reporting Timeline

- All incidents must be reported as soon as practicable and, wherever possible, within twenty-four (24) hours of becoming aware of the concern.
- Failure to report promptly may attract consequences as this may increase organizational risk and compromise legal, regulatory, or donor compliance obligations.

3.3 Protection of Whistleblowers

LISUDEV is committed to fostering a culture of transparency and accountability. Any individual who reports a concern in good faith is protected from retaliation, harassment, discrimination, victimization, or any adverse consequences resulting from such reporting, with procedures put in place in the whistleblower policy. However, making false, malicious, or misleading reports may result in disciplinary actions.

3.4 Investigation

All reports received must be reviewed promptly and confidentially. LISUDEV will conduct internal investigations; suspend payments or transactions pending review; notify donors and funding partners; report matters to relevant law enforcement or regulatory authorities; engage external auditors, legal counsel, or investigators; and implement corrective and disciplinary actions.

3.5 Related Procedures

Further guidance on reporting channels, investigation processes, due diligence requirements, documentation standards, and corrective actions is provided in the LISUDEV Anti-Terrorism and Anti-Money Laundering Procedures Manual and other related organizational policies.

4. RESPONSIBILITIES

Ensuring compliance with the Anti-Terrorism and Anti-Money Laundering Policy is the responsibility of every LISUDEV staff.

5. TRAINING

LISUDEV will provide regular training to its staff to ensure they understand their responsibilities, the risks of prohibited transactions and terrorist financing, how to minimise them and report suspicion.