Policy on Money Laundering & Terrorism Funding

Preamble

Understanding and witnessing the suffering of the Sri Lankan communities who were trapped into a bloody ruthless civil unrest caused by terror and counter-terror actions for a protracted period of 4 decades.

Taking into consideration the commitment and the courage showed by the International community and the Government of Sri Lanka in fighting terrorism at the global and national level.

Keeping in mind the consequences of terror on the vulnerable communities, the women, children, elders and marginalized communities.

Committed to a safer world and nation to all the people who aspire for a dignified life and prosperous future.

This policy document is articulated, printed and published by the department of Institutional security of the People's Solidarity Platform in October 2022.

1.Introduction

This policy is in reference with the sets of counter-terrorism laws and sanctions at the national and international level. The most influential instrument is the UN Security council resolution 1373 adopted in September 2001 following the 09/11 terror attacks in the United States.

It obliges the parties to implement measures to deny individuals or entities engaged in Terrorism directly or indirectly access to funds, financial assets, goods or services.

Along with the International convention for the suppression of the financing of Terrorism (One of 14 Multilateral treaties addressing different aspects of terror acts, the resolution has influenced much counter-terrorist law and practice at National levels. Significant non-legal measures include the UN General assembly Global counter-terrorism strategy and the Financial Action Task Force (FATF) an inter-governmental body established in 1989 to combat money laundering and terrorist financing.

This policy document is also in reference with the security arrangements enforced by the Government of Sri Lanka on monitoring of non-profits and foreign aid strictly enforced to tackle Money Laundering & Terrorism Funding.

The policy document draws attention to all the Civil society entities and non-profits to mobilize inclusive and joint efforts to confront the risks faced by the non-profits due to the challenges of money laundering and terrorism funding.

2.People's Solidarity Platform and Guiding Principles

People's Solidarity Platform is an impartial, neutral and independent humanitarian and development entity, which formulates its own policies and guiding principles to sphere-head its mission based on its strategic objectives.

This policy paper which expresses the platform's position on Money laundering & Terrorism Funding (ML&TF), allows the platform to maintain high ethical standards, protect its reputation and implement its humanitarian and development mandate.

This policy sets out the specific obligations and conditions related to Money Laundering and Terrorism Funding (ML&TF) to which the platform strictly adheres in conduct of its Mission.

This document will be communicated to all platform staff as well as to relevant partners and donors and other individuals and entities as needed. Staff who work in areas identified as particularly risk will receive additional training and support in addressing and reacting to potential terrorist activities and financing.

This policy applies to all individuals working at all levels, including partners, consultants, employees (fixed term or special service agreement) contractors, trainers, staff, volunteers or any other persons associated with the mission of the platform wherever located.

3.Position of People's Solidarity Platform

The Platform is committed to follow the national and international laws in executing its mission in its target and countries it operates.

The platform will acknowledge and adhere the counter terrorism legislations set up by the international community, donors, and the country of operation.

The platform will not promote or commit any act, which could be considered as act of terrorism by the UN Security council resolution 1566 (2004)

The platform will not provide assistance of any form, to any groups | individuals who does not/ or fails to adhere with the policies and procedures regarding to Money laundering and Terrorist Funding (ML&TF) and will not support groups or individuals considered as terror groups by the international community, donor or the country of operation.

The platform will not cooperate with any group or individual considered as Terror group by the International community, donor or country of operation.

The platform will not collaborate with known associates of any groups or individuals considered as Terrorists by the International community, donor and the country of operation.

The platform will not utilize its funds for any ventures or activities identified as risk to the National and International security mechanisms and will not finance any initiatives that are not related to the strategic benchmarks of the platform.

The platform will take all necessary precautions, not to expose its International and local staff to any danger in particular when working in areas or countries where the risk of terror activities are exacerbated.

The platform will stand committed to implement and practice this policy and will commit itself to review and seek recommendations from partners, communities, intellectual circles and state mechanisms on counter terrorism legally formed within the constitutional framework of the countries of operation to update this policy and stand dedicated to its effective practice by all individuals concerned and connected.

The platform is committed to continuous awareness of this policy to all its community target groups, stakeholders, staff, consultants and will provide continuous training and updates to its entire workforce.

Any viable information, reports, analysis regarding the breach of this policy or requirement of a rapid response, supervision or analysis must be immediately reported either to the department of institutional security headed by the Chief of Mission of the platform

4.Obligations and best practices

The platform is committed to meeting its regulatory obligations in identifying, mitigating and managing money laundering and terrorist financing risk that can impact on the organization's mission and its services to the communities. It seeks to protect the communities it serves, employees and stakeholders from the risks of ML&TF activities and recognizes that it plays a critical role in this regard by putting the necessary mechanisms and systems in place.

The platform continues to invest significantly in its fight against ML&TF and recognizes upgrading and enhancing its Human resources technology and systems.

These are the key areas the platform focuses to actively engage its stakeholders into the process of implementing its recognized policies.

A. Communication

The departments of Institutional security of the platform strongly feel that effective sharing of information within the organization and among its stakeholders are viable to engage people in implementing this policy and we concentrate on the following approaches and mechanisms.

1. Orientation and Training to the staff on the policy and integrating the policy document as an integral part of all contracts.
2. Sharing relevant information with all departments and follow up the viability of information flow
3. Share information regarding our policy on ML&TF to all our contractors, suppliers and partners
4. Establish contacts with legally established state counter-terrorism mechanisms for rapid information sharing
5. Document and share National and International resolutions, conventions and provisions.
6. Establish a data-base of the proscribed organizations and their counter-parts
7. Establish a communications protocol to the organization
8. Take up issues and find remedies and follow-up at the DIS meeting

B. Human Resources Management

Human Resources Management in this section refers to all the divisions that the organization has working relationship with and DIS expects that every single individual should transparently present information required by DIS before start of any business thereof.

1. Screening and documentation of all individuals (staff, trainers, suppliers) before entering into officials business (This includes obtaining report from the closest police station)
2. Elaborate clearly to all persons concerned regarding the ML&TF process within the entity.
3. Establish a workable training and capacity development calendar within the organization
4. Provide and update reliable information about staff to the state security mechanism to consolidate staff security.
5. Organize staff appraisals with a special focus on organization policies.

C. Technology and systems

Technology and systems refer to all the technicalities and systems both manual and electronical and paradigms used internal and external by the entity including the systems and peripherals used by the contractors, suppliers, trainers and staff.

1. Restore and maintain all the computers and peripherals, devices and equipment of the entity under the DIS and assign a focal point for system and cyber security.
2. Establish a rapid response communication system to mitigate risks and emergency planning

3. Store all the correspondence files under a safe system access to the DIS
4. Assign staff with clear ToR to handle the communication devices and systems
5. Have a clear protocol to trace the digital and social media accessories.
6. Have a clear system to document, account and reconcile the effective.
7. Establish a financial governance and partner management system.
8. Conducts regular risk analysis concerning anti-terrorism activities. The risk analysis typically includes a review of the relevant legal requirements of donor governments, transit governments (e.g., territories through which goods or services are transferred), and host state governments, as well as donor policies and industry standards (if any) from other sectors. It also includes security analyses, including stakeholder analyses (armed groups, state and non-state actors), to determine the risk of terrorism targeting or undermining our operations.
9. Enforces a strict code of conduct among its staff and staff of partner organizations with a strong reference point to anti-diversion and a statement on financial transactions with armed groups.
10. Maintains comprehensive financial records which account for all expenditure and publishes annual financial statements with detailed breakdown of incomes and expenditures.
11. Conducts annual external audit of all expenses as well as external audits of specific projects. Reserves the right to carry out Third Party reference checks on individuals with whom the platform has or plans to have a contractual link to ensure these individuals are not associated with terrorism and do not appear on counter-terrorism lists through the use of an industry-standard auto-screening software.
12. Ensure training of its staff and partners on anti-diversion policies, procedures and practices.
13. Conducts an in-depth due diligence of partners and sub-grantees, including Third Party Reference Check to ensure the partner/sub-grantee does not appear on counter-terrorism lists through the use of an industry-standard auto-screening software.
14. Applies a "know your supplier" principle for procurements for all national, international and restricted tenders.

D. Finance transaction, Management and enforcement

1. The Supreme council of the platform and Country Focal Points are responsible for:

   Ensuring that the platform all staff members, volunteers & interns and contractors comply with all relevant legislation, platform's Code of Conduct and policies.

2. Ensuring that all partner organizations and their board members, staff members, volunteers and contractors implementing aid and development projects funded by or through the platform comply with all relevant legislation and policies.

3. Reporting to the DIS any information which could relate to breaches of this policy.

4. All employees, volunteers & interns are responsible for: Complying with this policy and other relevant legislation.

5. The platform's Human Resources Department is responsible for: Recruitment of employees, volunteers & interns, and any additional Third-party reference checks;

   Ensuring that each member of staff abides by the Code of Conduct of the platform

   Ensuring adherence to relevant data protection legislation;

   Providing support to managers and other staff during any complaint or dismissal Process
6. The platform's Security & Safety Focal Point is responsible for: Ensuring that up to date risk assessments and contextual analysis are provided for each area of intervention to determine risks (of aid diversion).
7. The platform's Finance Department is responsible for: Maintaining financial records and tracking all expenses and incomes: The platform maintains a multicurrency accounting system that allows tracking any expenses or incomes with a unique reference (voucher number) in the system. Each direct cost is linked to a specific project, contract and donor;
8. Controlling the use of the platform funds: through internal control mechanism as outlined in the platform's Finance manual and procedures; Selection of banks/financial institutions: following a due diligence check, incl. third party reference check;
9. Bank management: authorized levels to carry out financial operations, segregation of duties, signatures, monthly bank reconciliations contribute to having a clear picture on the use of funds and avoid misuse of funds;
10. Cash management: cash keeping processes, segregation of duties, monthly cash checking, contribute to having a clear picture on the use of funds and avoid misuse of funds;
11. Money transactions: Control done before payment: as defined in the platform's finance manual and procedures, no commitment of expense can be done without authorization, must be documented with both internal (validation of the expense beforehand, including purpose of the transaction and link to the budget line of the donor's contract) and external documentation (bill, receipt, proof that the service or good has been provided). Then only the expense can be done and booked in the system.
12. Bank transfers are preferred. In case of payment to be done in cash, a specific procedure has to be followed with identity check of the person coming to collect

the payment at the office. Following any payment by the platform, a confirmation of the receipt of funds is systematically requested.

13. Encourages stakeholders to report suspected terrorist activity using confidential means through a safe communication process.

Policy Review

The supreme Council and the management will work with all related stakeholders to establish a review process to this policy instrument, where the Supreme Council of the platform accepts feedbacks and scholarly inputs from all related stakeholders including the communities that we serve.

Feed backs and inputs can be mailed to dis@solidarity.lk with the Subject of Policy review inputs. Also visit www.solidarity.lk/policydesk for more related information.

This instrument was articulated by the Knowledge Management Unit of the People's Solidarity Platform and published by the Department of Institutional Security by the orders of the Supreme Council on the 17th day of October 2022.