ARPAN

ASSOCIATION FOR RURAL PLANNING AND ACTION

Anti-Money Laundering Policy

⚠️ Disclaimer

ARPAN
ASSOCIATION FOR RURAL PLANNING AND ACTION

ANTI-MONEY LAUNDERING POLICY

1. Introduction

1.1 Association for Rural Planning and Action (**"ARPAN"** the **"Organization"**) aims at highest ethical and moral standards in the professional and personal life of all associates. **ARPAN**'S Anti-Money Laundering Policy aims to ensure that the organization operates with, and is in compliance with applicable laws, regulations, ethical business practices, and is not used as a conduit for suspicious or money laundering activities or for funding illegal activities including the financing of terrorism.

2. Applicability

2.1 This Policy applies to all Employees/staff on rolls of the Organization, Trustees, Directors, Consultants and third parties such as volunteers, interns acting on our behalf (**"Associates"**) while discharging their functions and should be read in conjunction with the existing applicable laws and guidelines, as issued by relevant statutory authorities from time to time.

3. Background

3.1 'Money Laundering' is the processing of criminal proceeds[1] i.e. money generated from criminal acts *inter alia* drug and human trafficking, terrorism, smuggling, corruption, tax evasion, sale of weapons, organized crime, fraud and many other crimes with the objective of hiding its source and rendering it in legally usable form. It is any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. The process involves creating a web of financial transactions so as to hide the origin ownership and true nature of these funds. These proceeds may also be exchanged for money or assets that are 'clean'.

3.2 'Terrorist financing' is the use of legally or illegally obtained funds to facilitate terrorist activities and organizations. Money laundering and terrorist financing may involve a wide variety of financial products, services, and transactions including lending and investment products, and the financing of equipment and other property that could be used to facilitate terrorism and other criminal activity.

3.3 Money laundering is largely understood to mean any act or attempt (directly or indirectly and even by association and assistance in one step or a series of transactions) to convert, move, transfer, use, possess, acquire proceeds from illegal/criminal origins or assisting persons in doing it so that they appear to be legally acquired; thereby avoiding the detection, prosecution, conviction and confiscation of such proceeds. It includes terrorist organizations, tax evaders, smugglers,

persons involved in bribery or any persons that becomes aware of, or suspects that the money they have used or received is derived from illegal activities and/or through illegal means.

3.4 Generally, the money laundering process involves three (3) stages: placement, layering and integration. As illegal funds move from the placement stage through the integration stage, they become increasingly harder to detect and trace back to the illegal source.

- **Placement:** The stage where funds generated from illegal/criminal activities, commonly in the form of cash, first enter the financial system. This may be done by making deposits with financial institutions or converting the proceeds into negotiable instruments.
- **Layering:** After illegal funds have entered the financial system, layers are created by closing and opening bank accounts, purchasing and selling various financial products, transferring funds among financial institutions and across national borders. The criminal's goal is to create layers of transactions to make it difficult to trace the illegal origin of the funds.
- **Integration:** When the criminal believes that there are sufficient number of layers hiding the origin of the illegal funds, they reintroduce and safely invest the funds or apply them towards purchasing a legitimate service or asset in the economy, fund legitimate businesses, or conduct other criminal activity.

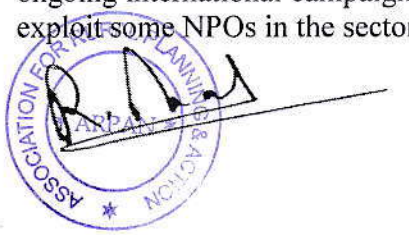
4. Money Laundering and Non-Profit Organizations

4.1 India is amongst the six countries that are being actively monitored by Interpol and International banking watchdogs after the detection of massive money-laundering cases in the last few years due to inadequate internal compliance procedures.

4.2 Nonprofit organizations (**"NPOs"**) play a pivotal role in many national economies and social systems. As per Rule 2(cf), PMLA Rules, NPOs are organizations that are registered as a trust or societies. For the purposes of Recommendation, NPO is referred to as a legal person or arrangement or an organization that primarily engages in raising or disbursing funds for charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".

4.3 The Financial Action Task Force (**"FATF"**), an intergovernmental international organization, recognizes the vital importance of NPOs in providing charitable services, as well as the difficulty of providing assistance to those in need, often in high risk areas and conflict zones, and applauds the efforts of NPOs to meet such needs. The FATF also recognizes the intent and efforts of NPOs to promote transparency within their operations and to prevent terrorist financing, including through the development of programmers aimed at discouraging radicalization and violent extremism.

4.4 Despite these efforts, NPOs are particularly vulnerable to be misused to raise and move proceeds, provide logistical support, and to facilitate terrorist activities and operations. The ongoing international campaign against terrorist financing has identified cases in which terrorists exploit some NPOs in the sector as a front for money laundering.



Thus, protecting NPOs from terrorist financing abuse is both a critical component of the global fight against terrorism, and a necessary step to preserve the integrity of NPOs and the donor community. Measures to protect NPOs from potential terrorist financing abuse should be adopted and be in line with the risk-based approach. Further, since NPO's catch the attention of philanthropists as well as thieves alike, it is becoming necessary that NPO's be monitored with respect to their source of funds, its utilization, purposes for which they were formed and the persons who carry out these activities. The FATF has therefore paid special attention to the NPO sector realizing the grey areas in NPOs and laid down Recommendation 8, "Combating abuse of Non Profit Organizations" **("Recommendation")** [2].

4.5 Since becoming a part of the FATF in 2010, India has accorded the Recommendation 8 into reality. Finance Intelligence Unit – India (**"FIU-IND"**) has prescribed filing of a separate report for Reporting Entities (banks, insurance companies, stock market intermediaries) for filing details of transactions carried out by NPO's. Also, basis the Recommendations, India undertook a series of amendments in the FCRA laws (including the 2020 amendments) to ensure that the money laundering risk is curbed and adequately addressed in the NPO sector.

4.6 Prevention of Money Laundering Act, 2002 (**"Act"**), was also enacted to aptly cover the reporting and monitoring obligations of entities and organizations covered therein. By way of the Gazette Notification dated 12th November 2009, the Act was enhanced to cover the NPO's in India. NPO's are required to adhere strictly to Know-Your-Customer **("KYC")** norms in case of any donations they receive, according to banking standards, and will have to regularly maintain detailed statements of their funds received and investments made.[3]

5. Policy Statement

5.1 **ARPAN** has resolved that it would, as an internal policy, take adequate measures to prevent money laundering and shall put in place a framework to identify, monitor and report suspected money laundering or terrorist financing transactions to FIU IND as per the guidelines of the Act and Prevention of Money Laundering Rules, 2005 as amended from time to time **("Rules")**.

6. Scope & Objective of this Policy

6.1 Indian NPOs may become target for laundering the money because of several reasons, though one of the most significant reason is the Income tax benefits available to Indian NPOs involved in charitable activities. Income derived from property registered as a Trust, wholly for charitable or religious purposes is exempt from payment of taxes to the extent such income is utilized towards the objects of the Trust in India.

6.2 The objective of this Policy framework is to:

i. To create awareness and provide clarity on KYC standards and Anti-money laundering measures in the Organization;

ii. To follow proper Donor Due Diligence (DDD) procedures before registering them;

iii. To monitor financial activities, conduct regular scrutiny of the transactions involved and maintain records of all financial transactions involving receipts of more than Rs. 10 lakh, or its equivalent in foreign currency as in accordance with Rule 3(1)(BA), PMLA Rules 2005;

iv. To maintain records of cash donations received from the same donor or donors connected with each other within a given financial year, and as a practice to insist upon electronic payments;

v. To monitor and report suspicious financial transactions;

vi. To discourage and identify money laundering or terrorist financing activities;

vii. To take adequate and appropriate measures to implement and comply with the Act and other regulations in force from time to time, and establish processes to check and prevent breaches of such laws;

viii. To detect systemic 'Red Flags' regarding unacceptable or suspicious forms of payment;

ix. To ensure that the Organization is not involved in any transactions that are known or suspected to be means of laundering money. If any suspicious activity is noticed, Associates to promptly intimate the Chief Operations Officer **("COO")**.

7. Red-Flags

7.1 Recognizing transactions involving money laundering requires awareness of possible suspicious activities which may arise at any time. According to Rule 2(g), PMLA Rules, 2005, suspicious activities and transactions may include transactions and attempted transactions, in cash and other modalities, that give rise to reasonable suspicion that it may involve proceeds from illegal/criminal activities, are unusually or unjustifiably complex, serve no visible economic or lawful purpose, and/or are not for a bona fide purpose.

7.2 Below is an indicative list of actions about which Associates should be careful. This list is not exhaustive, as every circumstance is not foreseeable. However, regardless of appearing conjointly or individually, Associates need to be wary of the following situations that may be indicative of money laundering activities:

i. Donors/Users that are reluctant to provide complete information, and/or provide incomplete, false, or suspicious information, and/or are unwilling to comply with the Organizations identification requirements;

ii. Donors/Users that appear as agents or representatives for other individuals or organizations, but are reluctant and/or unwilling to provide complete information about such individuals or organizations;

iii. Any person, including an Associate, that is concerned about or insists on avoiding any reporting requirements required by law or refuses to maintain records mandated by law;

iv. High volume payments made in cash or cash equivalents only (such as money orders, traveler's cheques, internet currencies or prepaid cash cards) that are commonly used for laundering money;

v. Donations of large amounts that appear to be out of place or inconsistent with normal donation patterns, in the absence of any legitimate purpose for such donation. For instance, particular Donor donates a substantially high amount in 2021, as compared to past 5 years while the project and purpose remained same;

vi. Requests for payments to be made through unrelated countries or to unrelated third parties;

vii. Multiple partial payments from various parties on behalf of a single user and/or multiple partial payments from various locations;

viii. Donors/Users making payments in one form, then requesting refunds in other forms (for example, making payments by credit card, but requesting refunds in cash or by wire transfers);

ix. Donors/Users making contributions, followed by immediate requests to wire out or transfer the funds to a third party or firm, without connected purposes;

x. Users requesting for donations to be paid in cash or wired to a third party or firm, without connected purposes;

xi. Donors/Users connected to countries and/or persons identified as non- cooperative by the Reserve Bank of India, Financial Action Task Force[4] on Money Laundering established by the G-7 Summit in 1987, Office of Foreign Assets Control, US Department of Treasury and international organizations against money laundering. A list of black listed and grey listed countries (countries and territories having "significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation) have been included as **Annexure A- 1**;

xii. Where the acceptance of foreign contribution is not prohibited under Sec. 12(4) FCRA, 2010. FCRA. The list of circumstances where acceptance of foreign contribution has been prohibited under this Act has been included as **Annexure A- 2;**

xiii. A donor makes a large contribution which does not seem to be commensurate with the donor's known background or income;

xiv. Unusual or substantial one-off donations;

xv. A donation that appears to be funded by someone other than the donor (eg. Donation is made by a cheque drawn on an account in the name of someone who is not a donor);

xvi. Conditions are attached to a donation which would mean that **ARPAN** is being used as a vehicle for transferring funds from one individual or organization to another without the trustees being able to verify that the donation is being put to an appropriate use;

xvii. Corporate donations made using a personal account, as in that case the donation will have to be returned and accepted through corporate account;

xviii. A beneficiary that is a shell company or that is established as a trust, is unwilling to provide additional information about its beneficial owners or underlying beneficiaries in response to a request for such information.

8. Checks to be observed

8.1 Associates must ensure that the Organization is in no way involved in any activity that falls under money laundering activities and that the Organization is not used as a conduit for transferring funds to a third person. Organization needs to adopt the following **"know-your"** principles alongwith the KYC norms listed above:

- **Know Your Donor:** For instance, charities may be used by donors to launder proceeds from a crime, or stolen credit cards may be used to make a donation to test whether it still operates. A template for a Donor Declaration Form has been attached in **Annexure A- 3.**
- **Know Your Beneficiaries:** For instance, false grant applications or inflated/false numbers of beneficiaries may be provided for claims and to undertake identity fraud in.
- **Know Your Partner:** For instance, false or inflated purchase orders for funds may be submitted to be paid for by NPOs.

8.2 These 'know-your' principles also complement and are in line with the Recommendations which require that **"NPOs should make best efforts to confirm the identity, credentials and good standing of their beneficiaries and associates undertake best efforts to document the identity of their significant donors".**

8.3 The following are the core elements of 'Know-your Customer' that must be satisfied by the Organization:

- **Identify the Donor** - know who your donor is by collecting their government issued identity proofs- Aadhaar and PAN, and filling of the Donor Declaration Form (attached in Annexure A-3).
- **Verify their Identity** – by carrying out appropriate checks from government portals like MCA, government identity proofs, donor's website, and filling of the Donor Due Diligence Form (attached in Annexure A-4)
- **Know their business-** to be assured this is an appropriate and legitimate organization for us to be involved with by verifying their terms of operation.
- **Know their business with the Organization** – to ensure that any individuals, contracts, MoUs, and business are not influenced directly or indirectly by the receipt of the donation.
- **Watch for unusual or suspicious activities** – so that any transactions, conduct, requests, or activities that qualify as red flags are not created by the Organization.

9. Steps to Ensure Compliance

9.1 Compliance with Applicable Law: Users/Donors must at all times, ensure that they access and/or utilize **ARPAN**'s platform in compliance will all applicable laws. Users contributing or donating should also ensure that funds used to contribute or donate to a campaign should not originate from any unlawful activity. Similarly, it must be ensured that the funds collected for a campaign should only be used for the purpose and objects specifically agreed between the parties. Relevant terms and conditions should be incorporated as part of the Donations form in case of sundry Donors, and the Donor due-diligence form, in case of Institutional Donors.

ASSOCIATION FOR RURAL PLANNING & ACTION * ARPAN *

9.2 Maintenance and Disclosure of Records: ARPAN shall maintain complete and accurate records confirming the identity of its Donors/users and the transactions undertaken in such a manner, intervals and maintain the records till such time-period as is specified under the applicable regulations. **ARPAN** will also disclose the information to government authorities, as required under the Act or in case of any inquiry, investigation or other proceedings initiated by them. **Additionally, as per the amended Rules and RBI Guidelines[5] issued from time to time, Banks are responsible to maintain a record of all transactions involving receipts by NPOs of value more than Rupees Ten lakh, or its equivalent in foreign currency to forward to the FIU-IND every month.[6] This report is called as Non-Profit Organizations Transaction Report (NTR). Detailed information on submission of the NTR is provided under Annexure A – 5 of this Policy document.**

9.3 Reporting Suspicious Activity: Any suspicious activity or red flag that **ARPAN** comes across must be reported to the **Chief Functionary, Renu Thakur** at **arpanuk.pith@gmail.com** or +91 9756605817 who shall take prompt and necessary actions in this regard and report to the FIU.

10. Amendment and Modification

10.1 ARPAN reserves the right to modify and amend this Policy at any time. Associates are advised to review **ARPAN**'s AML Policy from time to time, for the most up-to-date version.

11. Violations of this Policy

11.1 An Associate who violates this Policy or knowingly engages in activities specifically prohibited under this Policy, regardless of whether financial loss to the Organization results or not, may be subject to appropriate disciplinary action up to, and including termination. This shall be in addition to other rights and remedies available under the applicable laws.

12. Governing Law

12.1 Any dispute or claim relating in any way to this Policy is subject to the exclusive jurisdiction of the courts in **Pithoragarh**. Laws prevailing in India, without regard to principles of conflict of laws, will govern this Policy and any dispute related to/arising from this Policy, between **ARPAN** and the concerned Donor/user.