ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM POLICY

Effective December 17, 2021

I. PURPOSE & SCOPE

As a nonprofit corporation that operates globally, there is a risk that individuals or other organizations may attempt to use RMI to finance and support terrorist activity, violent extremism, or that other criminals or criminal organizations may attempt to launder money to legitimize proceeds from committing crimes. RMI makes all reasonable efforts to ensure that its projects and programs are conducted in accordance with all applicable laws and regulations, including sanctions programs administered by the Office of Foreign Assets Control (OFAC), and consistent with recommended guidelines to ensure that its funds and resources are not being used, directly or indirectly, to support terrorist activities, money laundering, or other Criminal Misuse of Funds.

This Policy applies to all RMI employees worldwide and to all RMI agents, representatives, Grantees, Collaborators, Service Providers, and all those with whom a business relationship is established.

II. POLICY

1. Organizational Integrity

RMI operates in accordance with its governing documents. These documents delineate RMI's basic goals and purpose; define the structure of RMI, including the composition of its Board of Trustees ("the Board"), how the members are selected and replaced, and the authority and responsibilities of the Board; set forth requirements concerning financial reporting, accountability, and practices for solicitation and distribution of funds; and confirm that RMI shall comply with all applicable local, state, and federal laws and regulations.

The Board is responsible for RMI's compliance with applicable laws, its finance and accounting practices and the adoption, implementation and oversight of practices, including financial recordkeeping to effectively safeguard RMI's assets. The Board maintains records of its decisions; maintains and makes publicly available a current list of its members, and privately maintains records of identifying information about the members of the Board. RMI also maintains records containing identifying information about its key employees and the key employees of any subsidiaries receiving funding from RMI.

2. Financial Accountability and Transparency

RMI prevents financial abuse and misuse of resources and funds by establishing strong financial controls and procedures. RMI has a budget that is adopted on an annual basis and is approved and overseen by the Board of Trustees. RMI's Chief Financial Officer is responsible for day-to-day oversight and control of RMI's assets. RMI keeps adequate and complete financial records of income, expenses, and financial transactions throughout its operations, including the end use of funds. RMI clearly states program goals when collecting funds and makes reasonable efforts to ensure that funds are applied as intended. Information about RMI's activities is publicly available. An independent certified public accounting firm audits RMI's finances and issues a publicly available, audited financial statement on an annual basis. RMI is informed as to the sources of its income and has established criteria to determine whether donations should be accepted or refused.

3. Relationship Management

To prevent the abuse of funds and resources by others, RMI carries out appropriate due diligence on its Donors*, Grantees, Collaborators, and Service Providers (collectively referred to as Stakeholders) before entering into a

written partnership or agreement. RMI verifies reputations of its Stakeholders through the gathering of publicly available information and completion of a vetting process. RMI applies a risk-based approach, particularly with respect to engagement with foreign Stakeholders due to increased risks associated with overseas charitable activity. Therefore, depending on the risk profile and type of Stakeholder, all the following steps may not be necessary and/or may not apply.

1. RMI will collect some or all the following basic information about a Stakeholder:
    a) The name of the Stakeholder in English, in the language of origin and any acronym or other names used to identify the Stakeholder;
    b) The jurisdictions in which the Stakeholder maintains a physical presence;
    c) Any reasonably available historical information that verifies the Stakeholder's identity and integrity, including: (i) the jurisdiction in which a Stakeholder organization is incorporated or formed; (ii) copies of incorporating or other governing instruments; (iii) information on the individuals who formed and operate the organization; and (iv) information relating to the Stakeholder's operating history;
    d) The available postal, email and URL addresses and phone number of each place of business of the Stakeholder;
    e) A statement of the Stakeholder's principal purpose;
    f) The names and available postal, email and URL addresses of individuals, entities, or organizations to which the Stakeholder currently provides or proposes to provide funding, services, or material support, to the extent reasonably discoverable;
    g) Copies of any public filings or releases made by the Stakeholder, including the most recent official registry documents, annual reports, and annual filings with the pertinent government, as applicable; and
    h) The Stakeholder's sources of income, such as official funding, private endowments, and commercial activities.

2. Once the appropriate information has been collected, RMI will complete the following vetting procedure before entering into any agreement or relationship with the Stakeholder:
    a) Conduct a reasonable search of publicly available information, including but not limited to the Terrorist Inclusion List ("TIL") to determine whether the Stakeholder is suspected of activity relating to terrorism, including terrorist financing or other support;
    b) Verify that the Stakeholder is not on the Specially Designated Nationals and Blocked Persons List (the "SDN List") maintained by OFAC at https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists and is not otherwise subject to OFAC sanctions;
    c) Confirm that the Stakeholder has the ability to protect funds or other resources that will be provided by RMI from diversion or exploitation by terrorist organizations and/or their support networks;
    d) In connection with funding from the USAID, verify that the Stakeholder is not included in any information concerning prohibited individuals or entities provided by USAID;

e) Verify that the Stakeholder has not been designated by the United Nations Security Council ("UNSC") sanctions committee;

f) If the Stakeholder is operating in a foreign jurisdiction, confirm the Stakeholder does not appear on a list of designated terrorist-related individuals maintained by that foreign jurisdiction;

g) Conduct a reasonable search of publicly available information regarding a Stakeholder's key employees, members of the governing board or other senior management to ensure such parties are not reasonably suspected of activity relating to terrorism, including terrorist financing or other support; and

h) Consider all information about the Stakeholder of which RMI is aware and/or is reasonably available.

3. Prior to disbursing funds or other resources, RMI will require a Grantee or Service Provider to certify that it is in compliance with all laws, statutes, and regulations restricting U.S. persons from dealing with any individuals, entities, or groups subject to OFAC sanctions, or, in the case of a foreign Grantee or Service Provider, that the Grantee or Service Provider does not deal with any individuals, entities, or groups subject to OFAC sanctions or any other persons known to the foreign Grantee or Service Provider to support terrorism or to have violated OFAC sanctions.

4. Program Verification and Management

When supplying monetary and in-kind contributions and other charitable resources, RMI has internal controls and monitoring systems to ensure that funds and resources are being used as intended. While these measures are primarily aimed at combatting money laundering and other financial crimes, they also serve to mitigate terror abuse by enhancing transparency and integrity of RMI in its operations and flow of funds and resources.

RMI's internal controls and monitoring systems include the following:

1. Confirming that the Grantee has the ability to both accomplish the charitable purpose of the Grant and protect the resources from diversion to non-charitable purposes;
2. Memorializing the terms of the Grant in a written agreement signed by both RMI and the Grantee which includes expectations and responsibilities of the Grantee, information as to the application of funds or other resources, and requirements for regular reporting, audits and on-site visits;
3. Monitoring the activities funded under the Grant on an ongoing basis during the Grant term to ensure funds and/or other resources are used as intended;
4. Requiring the Grantee to (a) take reasonable steps to ensure that the Grant funds or other resources are neither distributed to terrorists or their support networks nor used for activities that support terrorism or terrorist organizations and (b) apprise RMI of the steps taken to satisfy this requirement;
5. Auditing the Grantee to the extent reasonable – consistent with the size of the disbursement, the cost of the audit, and the risks of diversion or abuse of charitable resources – to ensure that the Grantee has taken adequate measures to protect its charitable resources from diversion to, or abuse or influence by, terrorists or their support networks; and
6. Requiring the Grantee to correct any misuse of resources and terminate the relationship should misuse continue.

5. Reporting Suspected Activity of Terrorism

Should the foregoing procedures lead to a finding that any Stakeholder or any of RMI's own key employees, members of the Board, or other senior management is suspected of activity relating to Criminal Misuse of Funds, including money laundering and terrorist financing, RMI shall take one of the following two courses of action:

1. If RMI believes there is a match between the name of a Stakeholder or individual(s) associated with RMI listed above and a name on the SDN List, RMI will follow the steps outlined by the OFAC to ascertain whether the match is valid as set forth at https://home.treasury.gov/policy-issues/financial-sanctions/contact-ofac/when-should-i-call-the-ofac-hotline or as otherwise published by the OFAC.

2. If RMI has information regarding suspicious activity relating to Criminal Misuse of Funds or terrorism which does not directly involve an OFAC match, RMI will disclose the activity to the US Department of the Treasury or the Federal Bureau of Investigation and to Stakeholders if such disclosure is contractually required.

III. DEFINITIONS

Term	Definition
"Collaborator(s)"	Organizations and/or individuals RMI partners with or works closely with
"Criminal Misuse of Funds"	Includes money laundering activities, the commission of underlying predicate crimes and all other unlawful uses or receipt of resources
"Grant"	A form of agreement with a Grantee that may be referred to as a Grant, subgrant, subaward or subrecipient agreement
"Grantee(s)"	Organizations RMI provides resources to in the form of a Grant
"Money Laundering"	Generally, refers to financial transactions in which criminals, including terrorist organizations, attempt to disguise the proceeds, sources or nature of their illicit activities
"Service Providers"	Organizations and/or individuals retained to provide services to RMI
"Stakeholders"	Collective way to refer to Donors, Grantees, Collaborators, and Service Providers
"Terrorism"	Any violent act, or a threat to commit such an act, that is done with the intention to coerce or influence a civilian population or government through intimidation

IV. RELATIONSHIP TO OTHER POLICIES & PROCEDURES

RMI maintains the following policies and procedures, which must be adhered to in conjunction with this policy:

- Gift Acceptance Policy
- Procurement Policy and Procedures

- Conflict of Interest Policy
- Anti-Bribery, Anti-Corruption, and Anti-Fraud Policy

V. POLICY REVIEW

This Policy will be reviewed every two years by RMI's Chief Financial Officer (CFO) and/or Legal Department, as needed. Changes to the Policy will be recommended to and approved by the Executive Council of the organization. Approved revisions shall be distributed to the organization by the CFO.

VI. OWNER and REVISION HISTORY

Owners: Legal Department and Accounting Department

REVISION DATE	KEY REVISION(S) MADE
12/17/2021	Policy approved by RMI's Executive Council