MAA INTERNATIONAL

COUNTER TERRORISM FINANCING POLICY

Work Product Unique ID: POL-CMP001

Version 3.5, Effective Immediately

TABLE OF CONTENTS

1 INTRODUCTION

MAA takes the issues of terrorism, money laundering, corruption, and fraud very seriously. MAA has a zero-tolerance approach to dealing with organisations or individuals who are involved in such unlawful activities.

The rise in global terrorism increases a number of associated risks, including that legitimate public or private funding can be diverted to support terrorist purposes. This can include charitable funds donated through Non-Profit Organizations (NPOs). Although rare, there are cases where NPOs have been used to raise, transfer and divert funds for terrorist purposes. There are a number of ways that terrorists can attempt to divert funds, including by fraudulently posing as legitimate suppliers, companies, NPOs and charities or by infiltrating legitimate enterprises.

Australian law prohibits the financing and support of terrorism, with offences applying under the Criminal Code Act 1995 (Cth) and the Charter of the United Nations Act 1945 (Cth) and associated regulations. Offences can apply regardless of whether the conduct constituting the offence or the result of the conduct occurs within Australia or overseas.

The consequences of becoming involved in terrorist financing are significant, and can include loss of reputation, status and donor confidence. Individuals or organisations, including NPOs, may face criminal penalties if they are found to have provided financial support to a proscribed individual or organisation or terrorist act.

NPO's should identify the specific risks to their organisation and, on that basis, form an opinion on the level of risk (e.g. high, medium or low). In particular, NPO's face a higher risk if they conduct or contribute to aid programs or projects overseas and/or donate funding to other NPOs or projects overseas, and/or work with, or provide funding to other NPOs that conduct programs or projects overseas.

It is important that NPOs regularly review their risks, particularly when there have been significant changes to the focus or scope of their activities.

This document contains MAA's Counter-Terrorism Policy.

1.1 PURPOSE

MAA renounces all forms of terrorism and will never knowingly support, tolerate or encourage terrorism or the activities of those who embrace terrorism and will make every effort to ensure that its resources are not used to facilitate terrorist activity.

This policy sets out MAA's response to the risk of dealing with individuals and organisations associated with terrorism and the Australian Government's legislation associated with this.

Relevant legislation can be found in:

- Part 5.3 of the Criminal Code Act 1995 ('the Criminal Code'); and
- Part 4 of the Charter of United Nations Act 1945 ('the UN Charter Act')

Failure to comply with Government requirements could significant impact the reputation of MAA as well as expose the organisation to potential penalties.

1.2 Policy Scope

MAA understands that terrorists use many means to finance their operations. This includes legitimate means, such as charities and donations, or illegitimate means, such as fraud, money-laundering, kidnapping for ransom and extortion. MAA also agrees with DFAT that 'it can be difficult to detect terrorism financing because it is covet in nature.

MAA is committed to endeavour to prevent any financing to terrorism as it is committed to carry on its core business operations of alleviating poverty, helping the poor and the needy, and saving the lives of vulnerable people in situations of emergency.

To achieve the both above-mentioned goals, MAA adopts the DFAT proportionate approach in its due-diligence practices. The proportional approach means to undertake 'reasonable efforts that are defined within an adequate risk management framework'. The world-class risk management framework presented in this document represent the basis of the MAA proportionate approach to counter Terrorism Financing.

In compliance with the United Nations Security Council sanctions regime and consistent with the Financial Action Task Force (FATF) recommendations, MAA does not partner with entities or individuals that participate in or support activities related to money laundering or financing of terrorism.

Due diligence is 'the check that is done before entering into an agreement', while Precautions is primarily about 'the ongoing management of risks throughout the lifespan of any activity'.
To that end, MAA undertakes the following activities/steps: -

1- Categorising the Field Partners and/or countries where MAA implements its aid programmes into two categories: Project Risk Ratings and Field Partner Membership Status.

   a. Project Risk-Ratings identify the risks associated with the project, location, and delivery challenges.

   b. The Field Partner Membership Status is based on assessing the partner's capabilities, reporting, policies, and financial risks.

c. The level of due diligence is proportionate to each category.

2- Placing subareas into the same two categories, where the subarea has a different categorisation that the main area.
3- Including in our funding agreement clauses to clarify MAA's and the Field-Partners', Suppliers' and subcontractors' obligations that better fulfils the intent of the legislative settings.
4- Undertaking pre-checks of all field-partners against the Listed Terrorist Organisations and the DFAT Consolidated List, i.e. the 'Proscribed Lists'. Also undertaking the same checks against the subcontractors, suppliers, sub-recipients, and field-partner directors in high-risk countries. All the results are kept in MAA's project/field-partner folders.
5- DFAT recommends checking Open Source intelligence (OSINT), such as the internet, social media and other screening tools.
6- Undertaking pre-checks for all MAA staff and volunteers. DFAT stated 'For tier 1 countries, we would like your organisation to ensure all sub-recipients' employees and volunteers are crosschecked against the proscribed lists, and use OSINT to inform decisions.'
7- Paying to close matches of names if they have the same date and place of birth.
8- Keeping log of all decisions made in blocking or removing the block of any partners or individuals.
9- In addition to the due-diligence checks that MAA conducts at the beginning with every new Field-Partner, Supplier and Subcontractors, MAA also conducts bi-annual checks against DFAT's proscribed list for Tier-1 countries.
10- MAA does not screen beneficiaries as it is extremely impractical to do so. However, in very particular situations when MAA would check a list of beneficiaries if valid concerns were brought to the attention of MAA.

1.3 Roles and Responsibilities

The following outlines MAA's responsibilities with regards to counter-terrorism risk:

1. MAA has a zero-tolerance approach to dealing with organisations or individuals who are involved in such unlawful activities;
2. MAA acknowledges that Australian Government legislation prohibits dealing with listed terrorist organizations and/or proscribed persons or entities. MAA undertakes due diligence checks in relevant databases provided by relevant government agencies to ensure MAA does not deal with such proscribed persons or organisations.
3. MAA will confirm the identity, credentials and good standing of the people or organizations it supports and will check that these people or organizations are not proscribed on the lists maintained by the Australian Government.

4. MAA will not knowingly remit any funds to known or suspected terrorist organizations or individuals.
5. MAA will report any known or suspected terrorist links to the relevant national authority.
6. MAA will use its best endeavours to ensure that overseas recipients of MAA's funds will adopt policies and procedures that enable them to comply with relevant Australian counter-terrorism laws.

1.4 DEFINITIONS

The following terms are used in this policy document and are defined as follows:

- ACFID: Australian Council for International Development
- DFAT: The Department of Foreign Affairs and Trade
- Government: The Australian Government
- Laws: means any relevant Australian laws, foreign laws, regulations and conventions designed and targeting terrorist cells and terrorism. [In Australia those Laws include but are not limited to, Commonwealth Criminal Code Act 1995, the Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Cth)]
- LinkMatchLite: The LinkMatchLite (LML) software is designed to assist asset holders in finding possible matches between their clients' names and names on the Consolidated List.
- Lists: means Department of Foreign Affairs and Trade, Government List and National Security lists regarding potential terrorist threats.
- NPO: Non-Profit Organisations
- Counterparty: Any third-party that contributes to, executes, implements, or in any way participates in MAA related activities, including procuring, giving or receiving of funds, services or supplies, or other form of support to or from MAA. Counterparties include Delivering Partners.
- Red flag: A term used to denote a warning signal or a sign of some problem requiring attention. Money laundering and financing of terrorism usually indicate red flags before they are committed. The red flags vary depending on the type of scheme.
- Due diligence: A process to identify, verify and validate the identity of the Counterparty. This enables MAA to assess and evaluate the extent of risk related to money laundering and financing of terrorism regarding the relationship with the prospective Counterparty.
- Risk: The effect of uncertainty on objectives (an effect can be negative threat or hazard, positive or opportunity a mixture of both) (deviation from what is expected) the possibility an event will occur, or circumstance will arise that affects the achievement of objectives.
- Risk-based approach: The process of identifying, assessing and understanding money laundering and financing of terrorism risks to which MAA is exposed and adoption of appropriate measures to mitigate the risk.
- Proscribed List: The government can list an organisation as a terrorist organisation if the Attorney- General is satisfied that it is engaged in preparing, planning, assisting or fostering the doing of a terrorist act or advocates the doing of a terrorist act.
- Terror Act: an act, or a threat to act, that meets both these criteria:

(a) it intends to coerce or influence the public or any government by intimidation to advance a political, religious or ideological cause.
(b) it causes one or more of the following: death, serious harm or danger to a person, serious damage to property, a serious risk to the health of safety of the public, serious interference with, disruption to, or destruction of critical infrastructure such as a telecommunications or electricity network.

- Terrorism: means the unlawful use or threatened use of force or violence by a person or an organization against people or property with the intention of intimidating or coercing societies, often for ideological or political reasons.

2 POLICY & PROCEDURES

2.1 POLICY STATEMENT

Terrorism is defined as the unlawful use or threatened use of force or violence by a person or an organisation against people or property with the intention of intimidating or coercing societies, often for ideological or political reasons.

MAA does not permit nor allow any form of terrorism or facilitation of terrorism of any proscribed entity, either through the activity of MAA itself, or any of its associated offices, partners, donors or associates.

MAA shall carry out all its responsibilities under the counter-terrorism laws promptly, thoroughly and accurately.

2.2 GUIDING PRINCIPLES

MAA believes that any form of terrorism is unacceptable and will not be tolerated. The following statements guide MAA's Counter-Terrorism Policy: -

1. The Australian Government can list an organisation as a terrorist organisation if it advocates terrorism or engages in preparing, planning, assisting or fostering the doing of a terrorist act.
2. Financing terrorism involves the intentional collection or provision of funds (including on behalf of another person) and recklessness as to whether the funds will be used to facilitate or engage in a terrorist act.
3. Before an organisation can be listed, the Attorney-General must be satisfied on reasonable grounds that the organisation is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act.
4. Providing support to a terrorist organisation means any support or resources that are intentionally provided to help the organisation prepare, plan, assist in or foster the doing of a terrorist act.
5. Prior to funding any organisation, details of funded entities and their office bearers will be compared to Australian Government lists of terrorist and proscribed organisations.
6. MAA recognizes its duty to report any known or suspected terrorist links to the relevant national authority.
7. Adherence to this CTP is a mandatory requirement for all staff and partner organisations.
8. MAA will ensure that all staff and relevant stakeholders are made aware of the CTP and their responsibilities.

2.3 GOVERNANCE

While fully respecting individual privacy rights, MAA shall maintain records of identifying information for the members of the governing boards of any subsidiaries or affiliates that are in receipt of funds. To the extent possible, MAA will conduct screening against the DFAT, Attorney General's Department, UN and US Treasury sanction lists to ensure that the members of the governing boards are not among the proscribed entities.

MAA is prohibited from transacting with individuals, companies and countries that are on prescribed Sanctions lists.

Checks will be performed against the Criminal Code list of terrorist organisations and the DFAT consolidated list of individuals and entities subject to targeted financial sanctions, as per the following:

- Asian Development Bank Sanction list
- Attorney General's Department List of Terrorist Organisations
- DFAT's Consolidated List
- World Bank Listing of Ineligible Firms
- UN Security Council Consolidated Sanctions
- US OFAC Consolidated List

The lists are consolidated in DFAT's program LinkMatchLite.

2.4 PROCEDURES

MAA shall adopt a risk-based approach when engaging Counterparties in order to combat financing of terrorism. This risk-based approach is the process of identifying, assessing and understanding financing of terrorism risks related to activities and areas where MAA is most exposed; and to take measures commensurate to those risks to mitigate them effectively.

To adequately manage the risk of financing of terrorism , MAA shall conduct risk-based screening of Counterparties to identify, assess and understand financing of terrorism risk and in accordance with the applicable due diligence protocol and requirements, before working with them as follows:

A. Due Diligence

MAA shall apply risk-based due diligence approach, informed by Counterparty type and context; to confirm, verify and validate the identity of a Counterparty and enable a reasonably informed decision regarding engaging with a party. This enables MAA, among other things, to

assess and evaluate the extent of risk related to financing of terrorism regarding the relationship with the prospective Counterparty.

MAA shall seek out relevant background and business intelligence information on potential partners in order to identify and assess red flags with an aim to preventing and/or putting mitigation measures in place to protect MAA from any possible harms.

B. Counterparty relationships

MAA shall take reasonable measures to duly assess the purpose, economic rationale and overall financing of terrorism and related integrity aspects of the Counterparty to avoid being involved in relationships that expose the organisation to risk.

MAA shall not engage with, and will terminate Counterparty relationships as follows:

- MAA shall not partner with Counterparties who are currently in the list of terrorist organisations and the DFAT consolidated list of individuals and entities subject to targeted financial sanctions.
- MAA will terminate the existing Counterparty relationship with Counterparties who do not cooperate with this policy.

C. Monitoring

Monitoring the status of Counterparties (not in the sanctions list) on an ongoing basis is a key objective to ensure that MAA engages only with reputable and financially stable service providers and safeguarding the organisation's financial assets.

D. Confidentiality

MAA shall ensure that all information on partners engagement, and transactions obtained in line with this policy requirement is kept confidential.

2.5 REPORTING

If MAA becomes aware, whether personally or through a third-party complaint, of any connection or allegation of a connection to terrorism or a proscribed entity of any program funded by MAA, the person shall promptly report the complaint to the CEO, **in-case of complaint against CEO allegation should be reported to Chairperson**.

In the event of any substantive concerns about any aspect of MAA's operations, or that of any of MAA's funded programs, in relation to anti-terrorism legislation, the **CEO (if against CEO, report directly to Chairperson)** shall inform the Board as soon as possible. Upon receipt of such a report, the Board may seek legal advice regarding its position and any legal obligation it may have to report the results of the review, including any recommendation to voluntarily disclose the information to the Australian Federal Police or Attorney General's Department and

any other relevant government body or agency that has authority over anti-terrorism legislation in that jurisdiction.

MAA standardise reporting across all organisations operating in tier 1 countries, given grantees and contractors are equally required to observe Australian laws. This includes, for example, ensuring all organisations complete a standard template provided by us when checking the proscribed lists. The following needs to be kept as a standard:

- a list of MAA's employees and volunteers;
- a list of MAA's sub-recipients, subcontractors and suppliers;
- evidence of a risk assessment or a fraud risk assessment, whichever is more relevant;
- information on the types of controls used to manage the risks; and
- evidence of capacity building activities, such as counter terrorism training for employees and volunteers.
- Any Instance of allegations could be reported to MAA via following communication mediums;
    - compliance@maainternational.org.au
    - +61 (2) 8016 9500
    - PO BOX 395 Bankstown, NSW, 2200

3 REVISION HISTORY

Document version details	
Version identifier:	V3.5
Date amended:	31 December 2025
Approved by CEO:	Ahmad Malas
Review date:	31 December 2026 or as required

ANNEX 1 COUNTER TERRORISM FINANCING FORM 1

FOR COMPLETION BY THE OFFICER SUSPICIOUS OF ACTIVITY:

CONFIDENTIAL

Report to CEO (if against CEO, report directly to Chairperson) money laundering activity

To: CEO (if against CEO, report directly to Chairperson)

From: _____

[insert name of employee]

Directorate: _____

[Insert post title and business unit]

Ext/Tel No: _____

URGENT YES/NO

Date by which response needed: _____

Details of suspected offence: _____

Names(s) and address(es) of person(s) involved:
[if a company/public body please include details of nature of business]

Nature, value and timing of activity involved:
[Please include full details e.g. what, when, where, how. Continue on a separate sheet if necessary]

Nature of suspicions regarding such activity:
[Please continue on a separate sheet if necessary]

Has any investigation been undertaken (as far as you are aware)? (Please tick the relevant box)

☐ Yes ☐ No

If yes, please include details below:

Have you discussed your suspicions with anyone else?

(Please tick the relevant box) ☐ Yes ☐ No

If yes, please specify below, explaining why such discussion was necessary:

Have you consulted any supervisory body guidance re money laundering? (e.g. the Law Society) [Please tick the relevant box]

☐ Yes ☐ No

If yes, please specify below:

Do you feel you have a reasonable excuse for not disclosing the matter to AUSTRAC? (e.g. are you a lawyer and wish to claim legal professional privilege? [Please tick the relevant box]

☐ Yes ☐ No

If yes, please set out full details below:

Signed: _____ **Dated:** _____

Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described.

THE FOLLOWING PART OF THIS FORM IS FOR COMPLETION BY THE CEO (if against CEO, report directly to Chairperson)

Date report received: _____

Date receipt of report acknowledged: _____

CONSIDERATION OF DISCLOSURE:

Action plan:

OUTCOME OF CONSIDERATION OF DISCLOSURE:

Are there reasonable grounds for suspecting money laundering activity?

If there are reasonable grounds for suspicion, will a report be made to AUSTRAC? [Please tick the relevant box] ☐ Yes ☐ No

If yes, please confirm date of report to AUSTRAC: _____ and complete the box below:

Details of liaison with AUSTRAC regarding the report:
Notice period: _____ to _____
Moratorium Period: _____ to _____

Is consent required from AUSTRAC to any ongoing or imminent transactions which would otherwise be prohibited acts? [Please tick the relevant box] ☐ Yes ☐ No

If yes, please confirm full details in the box below:

Date consent received from AUSTRAC: _____

Date consent given by you to employee: _____

If there are reasonable grounds to suspect money laundering, but you do not intend to report the matter to AUSTRAC, please set out below the reason(s) for non-disclosure:

[Please set out any reasonable excuse for non-disclosure]

Date consent given by you to employee for any prohibited act transactions to proceed:

_____

Other relevant information:

Signed: _____ Dated: _____

ANNEX 2 RED FLAGS

The risk indicators below are not intended to be exhaustive but to show a few potential signals of money laundering and financing of terrorism activities. Red flags are not sufficient basis to confirm the existence of money laundering or financing of terrorism activity. They only trigger further review, checks and verification to be satisfied that the transaction is not contributing to money laundering or funding of terrorism, in accordance with this policy.

a. The source of funds from a donor is suspicious - such as funds received from a high-risk entity (dubious reputation, unverified identity) or country with weak financial infrastructure, or donor with links to those that engage in or support money laundering activities or financing of terrorism, or large contributions in cash, not through the financial system.

b. Counterparty provides false or inconsistent information during the due diligence verification – this may include fake documents, email accounts that cannot be found on the internet and so on – provision of false or suspicious information should arouse further queries.

c. Counterparty is reluctant to provide needed information or data for due diligence verification. This could include refusal to provide details of principals or key management or those with majority interest in the entity.

d. Counterparty is overly secretive of the entity's business or evasive regarding their clienteles, beneficial owners among others.

e. Counterparty is using an agent or intermediary without adequate or logical justification or uses email address with unusual domain part.

f. Counterparty requests for partnership or services or transactions not compatible with those declared or not typical for that type of entity.

g. Counterparty requests to be paid in cash instead of bank-to-bank transfer. MAA procedure is to pay suppliers or implementing partners through the bank system.

h. Frequent changes of vendor's bank accounts by Counterparty without adequate justification. There are genuine reasons for changing bank accounts, however, when such request becomes frequent or urgent, special care should be taken prior to effecting the change.

i. Multiple bank accounts belonging to the same supplier or implementing partner without good reasons.

j. Request to pay a supplier or implementing partner through a third party. MAA process requires payments to be made directly to the service provider or

implementing partner unless "alternate payee" has been authorised by MAA management to that effect.

k. Structuring transactions to avoid government reporting, tax compliance or record keeping requirements.

l. Refunds from implementing partner using unusually complex structures that bear no connection with the implementing partners registration.

m. Refunds of programme funds in cash – programme refunds should be done through the bank.

n. Wire transfer activity that is not consistent with the business activities of a vendor, or which originates or terminates with parties unrelated to the transaction.

o. An unauthorised person acting as representative or signatory of a Counterparty, or a person claiming to be a representative but not ever listed or introduced as a formal party to the transaction or relationship.