

LANDMARK RELIEF INTERNATIONAL

Foundational Governance Policy

Partner Due Diligence Policy

Aligned with Canadian law (federal and Ontario)
and United Nations and international humanitarian standards
Effective date: October 7, 2026

About this policy

This document sets out the Partner Due Diligence Policy of Landmark Relief International (the "Organization"). It is one of three foundational governance policies, together with the Safeguarding Policy and the Complaints and Feedback Policy. Each policy is self contained and is adopted, versioned, and reviewed separately by the Board of Directors. Together they form the core of the Organization's accountability and risk management framework and are designed to satisfy the expectations of institutional donors and to align with the legal requirements of Canada, where the Organization is incorporated (at the federal level and in Ontario), as well as recognized United Nations and international humanitarian standards.

The legal instruments and standards this policy relies on are named at the end of the policy and listed in the References appendix, with enough citation detail for independent verification.

Partner Due Diligence Policy

Policy owner	Finance and Compliance Lead
Approved by	Board of Directors, Landmark Relief International
Version	1.1
Effective date	October 7, 2026
Review cycle	Every two years, or sooner following a regulatory change
Applies to	All implementing partners, sub grantees, and higher risk vendors and consultants

1. Purpose

Landmark Relief International works with partners to deliver its mission. This policy sets out the checks the Organization performs before and during a partnership to ensure that funds and assistance reach their intended purpose and are not diverted to terrorism, sanctioned parties, money laundering, fraud, or corruption, and that partners have the legal standing, financial controls, safeguarding capacity, and technical ability to deliver responsibly. Due diligence protects affected communities, the Organization's funds and reputation, and its legal standing in Canada.

2. Scope

This policy applies to all implementing partners and sub grantees that receive funds or deliver activities on the Organization's behalf, and to higher risk vendors and consultants. The depth of due diligence is proportionate to the assessed risk (see section 9).

3. Definitions

- **Partner:** any organization that receives funds from, or delivers activities on behalf of, the Organization.
- **Beneficial owner:** a natural person who ultimately owns or controls a partner organization.
- **Sanctioned or listed party:** any person or entity named on an applicable sanctions or terrorist entity list (see section 4b).
- **Politically exposed person (PEP):** a person entrusted with a prominent public function, whose involvement raises higher corruption risk.

4. Due diligence components

a. Legal status and governance

Verify the partner's legal registration, governing documents, board, key personnel, physical address, and good standing, and obtain audited accounts or financial statements where available.

b. Sanctions and counter terrorism screening

Screen the partner organization, its board members, senior management, and beneficial owners against the applicable lists before any agreement or transfer of funds, and re-screen periodically and before renewals:

- **Canada:** the list of terrorist entities established under section 83.05 of the Criminal Code and published by Public Safety Canada, and entities listed under the United Nations regulations and the Special Economic Measures Act.
- **United Nations:** the United Nations Security Council Consolidated List, including the ISIL (Da'esh) and Al-Qaida Sanctions List (resolutions 1267/1989/2253) and the 1988 (Taliban) Sanctions List.

- **United States (good practice):** the Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons List and Consolidated Sanctions List, including designations under Executive Order 13224, taking account of OFAC's 50 percent ownership rule. The Organization screens against these lists as a matter of good practice, because donors, financial institutions, and individuals associated with the Organization may be subject to United States sanctions.

The Organization immediately escalates any positive or possible match, pauses the transaction, and provides no funds or assistance until the match is resolved. The Organization does not enter or continue any partnership with a listed or sanctioned party.

c. Anti-money laundering and terrorist financing

Assess the source and flow of funds and the partner's financial controls, consistent with the principles of Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (administered by FINTRAC).

d. Anti-bribery and corruption

Require partners to comply with anti-bribery and anti-corruption law, including Canada's Corruption of Foreign Public Officials Act (CFPOA) and, where relevant to operations, other applicable anti-corruption laws such as the United States Foreign Corrupt Practices Act (FCPA) and the United Kingdom Bribery Act 2010. Facilitation payments, kickbacks, and bribes are prohibited.

e. Financial capacity and internal controls

Assess the partner's budgeting, accounting, procurement, segregation of duties, banking, and audit arrangements, and its capacity to manage and report on the funds proposed.

f. Safeguarding and PSEA capacity

Confirm that the partner has, or will adopt, safeguarding and PSEA policies, reporting mechanisms, and training equivalent to the Organization's Safeguarding Policy, and the capacity to apply them.

g. Technical and program capacity

Assess the partner's relevant experience, staffing, and systems for the activities proposed, and its monitoring, evaluation, accountability, and learning arrangements.

h. Conflict of interest and reputation

Check for conflicts of interest and adverse media or reputational concerns, and record any mitigations.

5. Documentation and records

Every assessment is documented on a standard due diligence form, with supporting evidence retained on file, a dated record of screening results, an overall risk rating, and a clear approval decision by an authorized officer. Records are retained for the period required by donors and applicable law.

6. Partner agreement requirements

Every partnership agreement includes flow-down clauses requiring the partner to:

- comply with all applicable sanctions and counter terrorism laws and warrant that it is not a listed or sanctioned party;
- comply with anti-bribery, anti-corruption, anti-fraud, and anti-money laundering laws;
- maintain safeguarding and PSEA standards and reporting equivalent to the Organization's;
- keep proper records, permit audits and site visits, and report promptly on funds and incidents; and
- accept suspension or termination and repayment of misused funds for breach of these obligations.

7. Ongoing monitoring and reassessment

Due diligence is not a one-time event. The Organization re-screens partners against sanctions and terrorist entity lists periodically and before renewals, monitors financial and program performance, follows up on audit findings and incidents, and updates the risk rating accordingly.

8. Red flags and escalation

- A screening match, or refusal to provide ownership or governance information.
- Requests to route funds through unrelated third parties or unusual jurisdictions.
- Missing registration, audited accounts, or basic financial controls.
- Adverse media, unresolved fraud, or safeguarding allegations.

Escalate any red flag to the Finance and Compliance Lead and, for terrorism, sanctions, or serious integrity concerns, to the Board, before the partnership proceeds.

9. Risk tiering

- **Lower risk:** established partner, small value, low risk context: core legal, sanctions, and safeguarding checks.
- **Medium risk:** new partner or moderate value or context: full component review under section 4.
- **Higher risk:** high value, higher risk context, or weak controls: enhanced due diligence, including beneficial ownership, enhanced screening, and closer monitoring.

10. Roles and responsibilities

- **Board of Directors:** owns this policy and receives escalations on terrorism, sanctions, and serious integrity risks.
- **Finance and Compliance Lead:** runs and records due diligence, screening, and approvals, and maintains the partner register.
- **Program leads:** assess technical capacity and support ongoing monitoring.

11. Legal and standards basis

This policy is grounded in: (Canada) the Anti-terrorism Act, 2001 and the Criminal Code terrorist entity listing regime (section 83.05) administered through Public Safety Canada, the Special Economic Measures Act, the Charities Registration (Security Information) Act, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (FINTRAC), and the Corruption of Foreign Public Officials Act; and (United Nations) the Security Council Consolidated Sanctions List. As a matter of good practice, the Organization also screens against the United States OFAC sanctions lists, including designations under Executive Order 13224. Full citations are in the References appendix.

12. Review

This policy is reviewed at least every two years and promptly after any relevant change in sanctions, counter terrorism, or anti corruption law.

References: legal and standards basis

The instruments below are the basis for this policy. They are current as of September 2026; sanctions and terrorist entity lists change frequently and must be checked against the official source at the time of each decision.

United Nations

- United Nations Security Council Consolidated Sanctions List, including the ISIL (Da'esh) and Al-Qaida Sanctions List (resolutions 1267, 1989, and 2253) and the 1988 (Taliban) Sanctions List.

Canada (federal)

- Anti-terrorism Act (S.C. 2001, c. 41; royal assent 18 December 2001), which added the terrorist entity listing regime to the Criminal Code.
- Criminal Code, section 83.05 (establishment of the list of terrorist entities), administered through Public Safety Canada.
- Charities Registration (Security Information) Act, S.C. 2001, c. 41, Part 6.
- Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17 (administered by FINTRAC).
- Corruption of Foreign Public Officials Act, S.C. 1998, c. 34.
- Special Economic Measures Act, S.C. 1992, c. 17.

United States (screening good practice and anti-corruption where relevant)

- Executive Order 13224 (23 September 2001), Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit, or Support Terrorism, administered by the Office of Foreign Assets Control (OFAC).
- OFAC Specially Designated Nationals and Blocked Persons List and Consolidated Sanctions List.
- Foreign Corrupt Practices Act (FCPA), 15 U.S.C. sections 78dd-1 and following.

United Kingdom

- Bribery Act 2010 (c. 23), where relevant to operations.