Moving Mountains Risk Management Policy

1. Purpose and Scope

This policy provides a structured framework for identifying, assessing, and managing operational threats to Moving Mountains Trust. It outlines how we proactively safeguard our assets, technology, and operations against major modern threats, specifically **cyber-attacks, funding losses, and international legal or compliance violations**.

This policy applies globally to all trustees, staff, volunteers, and our direct-implementation NGO partners in Kenya and Nepal.

2. Risk Management Framework

The charity utilizes a dynamic **Risk Register** to track threats. Risks are categorized based on their **Probability** (Likelihood) and **Impact** (Severity) on a scale of 1 to 5.

[Risk Identified] ⟶ [Assessed (Impact x Likelihood)] ⟶ [Mitigation Action] ⟶ [Quarterly Board Review]

The Board of Trustees holds ultimate accountability for the Risk Register, which is reviewed as a standing agenda item at every board meeting.

3. Cyber-Attacks and Information Security Risks

3.1 Digital Threat Context

As a small charity operating digital bank accounts (Ulster Bank and CAF), remittance platforms (Wise), and remote communications with Kenya and Nepal, we face risks from phishing, ransomware, identity theft, and fraudulent intercept of funding emails.

3.2 Mitigation and Controls

- **Multi-Factor Authentication (MFA):** Mandatory 2FA/MFA on all charity email, banking, Wise, and cloud storage systems.
- **Email Interception Safeguards (The "Voice Verification" Rule):** If an international partner requests a change of bank account details or a deviation in payment routing via email, **no funds will be transferred until the identity is verified via a live video or voice call** using a pre-known phone number. Email confirmations alone are never sufficient.

- **Software and Device Security:** All laptops and devices accessing charity data must have automatic operating system updates and active antivirus software enabled.
- **Data Backups:** All vital project files, financial logs, and legal data must be stored on encrypted cloud platforms (e.g., Google Workspace/Microsoft 365) to prevent total data loss in a ransomware attack.

4. Funding Loss and Financial Sustainability Risks

4.1 Financial Threat Context

Operating with an annual income under £250,000 means the charity is highly sensitive to the sudden withdrawal of a key donor, shifts in UK public giving, inflation, or severe exchange rate volatility affecting the Kenyan Shilling (KES) and Nepalese Rupee (NPR).

4.2 Mitigation and Controls

- **Income Diversification:** The charity must maintain at least three distinct funding streams (e.g., individual regular donors, trust/foundation grants, and community fundraising events) to ensure we do not depend on a single source for more than 50% of our total income.
- **Reserves Buffer:** A strict retention of **3 to 6 months of core running costs** in our CAF or Ulster Bank reserves account (as outlined in our Reserves Policy) to bridge sudden, temporary funding drops
- **Flexible Partner Contracts:** All Memorandums of Understanding (MoUs) signed with direct-implementation partners in Kenya and Nepal must include a **conditional funding clause**. This states that tranche disbursements are strictly subject to charity liquidity and can be scaled down or paused with 30 days' notice if funding collapses.

5. Legal, Regulatory, and Compliance Risks

5.1 Legal Threat Context

The charity must simultaneously satisfy conflicting regulatory frameworks across three distinct countries: the Charity Commission for Northern Ireland (CCNI) / HMRC in the UK, the NGOs Co-ordination Board in Kenya, and the Social Welfare Council (SWC) in Nepal. Non-compliance risks fines, operational bans, or loss of charity status.

5.2 Mitigation and Controls

- **Background Compliance:** Failure to vet staff or volunteers travelling to Kenya/Nepal poses extreme legal and reputational risks. Mandatory Enhanced Background checks are strictly enforced before any deployment.

- **Local Partner Vetting:** We mitigate international legal liability by strictly working with fully registered, compliant, local NGOs who handle their own local taxes and employment laws. Our MoUs dictate that they take full legal liability for local project implementation.
- **Sanctions and Anti-Terror Screening:** To ensure zero compliance violations under the UK Criminal Finances Act, the Treasurer must run the names of partner board members and key vendors through the UK Government's Office of Financial Sanctions Implementation (OFSI) screening list prior to disbursing funds.
- **Annual Legal Audit:** The Board will check the active registration status of our partner NGOs in Kenya and Nepal once a year to ensure they remain in good standing with their respective governments.

6. Incident Response and Business Continuity

If a major risk materializes (e.g., a total cyber breach or a massive loss of capital):

1. **Immediate Containment:** The Risk Lead takes immediate tactical action (e.g., freezing the compromised bank account or pausing a project tranche).
2. **Board Mobilization:** The Chair of Trustees calls an extraordinary board meeting within 48 hours to assess the damage and form a recovery plan.
3. **Statutory Reporting:** If the incident involves material loss of data, fraud, or a significant threat to operations, a **Significant Incident Report** will be submitted to the CCNI, and a data breach report will be sent to the ICO within 72 hours.

7. Review

The Board of Trustees will review this policy every two years, or earlier if legislation, CCNI guidance or the charity's activities change.