Risk Management Policy

Organisational risk assessment and response

Document ID	**RYO/POL/12/2026**
Document status	DRAFT TEXT - pending full-text Board ratification
Policy title endorsed	02 November 2026
Custodian	President / Head of Administration and Operations / Relevant function

This is a substantive working draft for RYO internal review. It is not evidence that these exact provisions were approved on 02 November 2026, when the policy titles were endorsed. Complete adoption requires a recorded competent-body decision.

1. Purpose and governance

RYO identifies, evaluates, treats and monitors risks to people, mission, funds, reputation, legal compliance, data and service continuity. The Board sets oversight expectations; the President leads strategic decisions; operations maintains the risk register and escalates high-severity issues.

2. Scope of risk

Consider safeguarding and PSEA, field/security conditions, financial fraud, donor noncompliance, staff capacity, procurement, adverse partnerships, data breaches, cybercrime, reputational events, educational quality, travel, physical assets and business continuity.

3. Risk assessment method

For each risk, record a description, cause, possible impact, likelihood, impact rating, existing safeguards, owner, treatment, target date and residual risk. A simple three-level likelihood and impact matrix can be used initially; serious safeguarding risks require prompt escalation regardless of score.

4. Risk appetite and escalation

No organisational benefit justifies deliberate harm to children or beneficiaries, sexual exploitation or abuse, bribery, corruption or unlawful acts. High risks, substantial losses and credible incidents concerning senior leadership must be escalated to non-conflicted decision makers and, where required, donors or authorities.

5. Safeguarding and duty of care

Programmes should assess travel, venue safety, participant age, recruitment/selection processes, transport, field supervision and digital communication. Protect the identity and safety of complainants and survivors, and maintain verified referral contacts for professional support.

6. Funding, program and partner risk

Review grant terms, dependence on a single donor, matching funds, milestone feasibility, subcontractor reputation and evidence needed to demonstrate results. No external partnership should be announced as official until appropriate agreements and authorisations exist.

7. Information security and business continuity

Maintain access controls, backups, device inventory, incident reporting, secure communications, and a recovery plan for essential contact, finance and programme records. Test backups and review access after staff changes.

8. Treatment, ownership and monitoring

Each risk is assigned to an accountable owner. Options include avoiding the activity, reducing exposure, transferring risk with legitimate insurance/agreements, or accepting a low residual risk with approval. The operations team reviews the register monthly; the Board receives a quarterly summary.

9. Incident management

For an incident, prioritise safety and containment, document who was notified, preserve evidence, appoint a non-conflicted reviewer and apply corrective action. Donor and legal notifications must follow applicable obligations. Record lessons learned without exposing protected personal data.

10. Review and reporting

Review the register whenever a new project, location, funding arrangement or major incident emerges. Update this policy at least annually.

Operational control table

Risk area	Example risk	Minimum mitigation
Safeguarding	Unsafe contact or exploitation	Screening, training, reporting routes
Finance	Misuse of funds	Authorisation and reconciliation
Projects	Donor deadlines missed	Milestone tracking and owner
Cyber and privacy	Loss of personal data	Access limits, backups, breach response
Staff and operations	Single person dependency	Handover and documented delegation
Partnership	Unverified or unauthorised commitments	Due diligence and signed mandates
Security	Unsafe movement or venue	Context-specific assessment and contingency

Implementation, approval and version control

Before this manual is applied as an official RYO policy, approve and record the full text and any internal threshold, signatory or role annexes; appoint its custodian; confirm training and operational readiness; and retain the authorised master version with the approval minutes. Review annually or on material changes.

Board ratification reference: _____ Effective date: _____

Authorised approval / custodian: _____ Version: 1.0 (draft)