Institutional governance and administrative operations regulations

GADIM REFUGEES EMPOWERMENT CENTER (GREC)

Republic of Uganda – Kampala

Adopted on 31 December 2025

Table of contents

Purpose of these regulations

These Regulations establish the Organization’s comprehensive institutional governance framework and translate the Constitution and the Board of Directors Rules of Procedure into practical rules and procedures governing authority, decision-making, oversight, accountability, risk management, compliance and institutional performance.

They ensure that administrative operations reflect the Organization’s vision, mission and strategic objectives and protect its independence, resources and beneficiaries.

PART I

PRINCIPLES OF INSTITUTIONAL GOVERNANCE

Article 1: Scope of Application

These Regulations apply to every person, body and activity falling within the Organization's governance and operational authority, namely:

- The General Assembly
- The Board of Directors
- Committees of the Board
- Executive Management
- Departments, offices, programs and projects
- Employees, volunteers and interns
- Consultants and contractors to the extent provided in their contracts
- Branch offices, missions and field teams
- Entities or initiatives managed or controlled by the Organization
- Every person or entity subject to these Regulations shall comply with them within the limits of the powers and responsibilities assigned to that person or entity.

Article 2: Governance Objectives

The Organization's governance system is intended to:

- Protect the Organization's mission, vision and values
- Ensure clarity of roles and authority
- Prevent the concentration of power in one person or body
- Strengthen oversight and institutional checks and balances
- Protect resources against corruption and misuse
- Ensure sound decision-making
- Promote participation and fair representation
- Protect beneficiaries from exploitation and abuse
- Improve performance and impact
- Strengthen the confidence of donors, partners and communities
- Support legal and regulatory compliance
- Build an institution capable of continuity and development.

Article 3: Governance Principles

Institutional governance shall be founded on the following principles:

- Legality: all authority shall be exercised in accordance with applicable law and the Constitution
- Accountability: every holder of authority shall be subject to review and evaluation

- Transparency: appropriate information shall be made available at the appropriate time
- Integrity: corruption, favoritism and abuse of influence shall be avoided
- Participation: stakeholders shall be involved in matters affecting them
- Fairness: persons shall be treated without unlawful discrimination or bias
- Independence: institutional decisions shall be protected from improper influence
- Efficiency: resources shall be used in the best possible manner
- Effectiveness: planned results and impact shall be achieved
- Sustainability: the Organization's capacity to pursue its mission shall be protected
- Do no harm: decisions that expose persons or communities to danger shall be avoided
- Accountability to affected populations: beneficiaries' rights to information, complaint and participation shall be respected.

Article 4: Governance Culture

Governance is not limited to formal rules and structures; it is an institutional culture that shall be reflected in the conduct of all staff, members and leaders. That culture includes:

- Accepting, rather than resisting, accountability
- Respecting dissenting views
- Discussing errors professionally
- Reporting risks early
- Not concealing material information
- Separating personal relationships from institutional decisions
- Encouraging learning and continuous improvement
- Prohibiting retaliation against good-faith whistleblowers or critics
- Prioritizing the interests of the organization and its beneficiaries
- Documenting decisions and the reasons for them.

PART II

GOVERNANCE STRUCTURE AND INSTITUTIONAL AUTHORITY

Article 5: Governance Structure

The institutional governance structure comprises:

- The General Assembly
- The Board of Directors
- Committees of the Board
- The Secretary-General
- Senior Executive Management
- Departments, offices and units
- Programmer and project teams
- Branch and field offices
- Specialized accountability and oversight committees
- Beneficiary and stakeholder participation mechanisms
- Each level shall operate within its mandate without exceeding or obstructing the mandate of another level, and in accordance with the hierarchy of authority and instruments prescribed by the Constitution.

Article 6: The General Assembly

The General Assembly is the supreme authority of the Organization and shall exercise the powers assigned to it by the Constitution.

Article 7: The Board of Directors

The Board of Directors is the body responsible for governance, strategic oversight and institutional control. It shall prepare the proposed strategic direction for approval by the General Assembly. The Board acts collectively, and no individual member may issue a binding decision unless formally authorized by the Board.

Article 8: Board Committees

Committees of the Board shall assist the Board in discharging its oversight and specialist responsibilities and shall operate under written terms of reference.

Article 9: The Secretary-General

The Secretary-General is the Chief Executive Officer of the Organization and is accountable to the Board of Directors. The Secretary-General shall implement approved strategy, plans, policies and decisions and manage day-to-day operations within delegated authority.

Article 10: Senior Executive Management

Senior Executive Management comprises the Secretary-General, the executive officer responsible for finance, and the heads of departments or other officers designated in the approved organizational structure.

PART III

DELEGATION OF AUTHORITY

Article 11: Principle of Delegation

Authority may be delegated to facilitate timely and efficient operations, if every delegation is:

- In writing
- Clear
- Limited in scope
- Time-bound where appropriate
- Consistent with applicable law and the constitution
- Subject to oversight
- Reviewable or revocable
- Proportionate to the responsibilities of the delegate
- Delegation does not relieve the original holder of authority of the duty to supervise and monitor its exercise.

Article 12: Delegation of Authority Matrix

The Organization shall adopt a written Delegation of Authority Matrix specifying, at a minimum:

- The type of decision
- The initiating body
- The reviewing body
- The approving body
- Financial thresholds
- Consultation requirements
- Documentation requirements
- Escalation circumstances
- The alternate authority during absence
- Conflict-of-interest restrictions
- The matrix shall cover finance, procurement, human resources, contracts, partnerships, programs and projects, travel, asset management, public communications, legal affairs, data management and emergencies.

Article 13: Sub-delegation

A delegate may not sub-delegate authority unless the original delegation expressly permits it, the sub-delegation is written and states its scope and duration, the original authority is notified, the delegate retains monitoring responsibility, and the arrangement does not weaken oversight or segregation of duties.

Article 14: Acting Appointments

Where an officer is absent or a position is temporarily vacant, an acting appointment may be made by written decision stating its duration, authority and limitations. The appointee shall be competent and free from conflicts of interest; relevant parties shall be informed; the appointment shall not circumvent permanent recruitment procedures; and a formal handover shall occur upon its conclusion.

Article 15: Review of Delegated Authority

The Delegation of Authority Matrix shall be reviewed at least annually and whenever there is:

- A change to the organizational structure
- The appointment of new leadership
- A material change in budget size
- An identified control deficiency
- Fraud or another material breach
- A new programmer or office
- A change in donor requirements or applicable law.

PART IV

INSTITUTIONAL DECISION-MAKING

Article 16: Decision-Making Standards

Institutional decisions shall be based on:

- A lawful or regulatory basis
- Sufficient and accurate information
- Risk analysis
- Assessment of financial implications
- Consideration of effects on beneficiaries
- Consultation with competent parties
- Evaluation of alternatives
- Disclosure of conflicts of interest
- Documented reasons
- Clear responsibility for implementation and follow-up.

Article 17: Classification of Decisions

Institutional decisions shall be classified as:

- Strategic decisions concerning the mission or long-term direction
- Governance decisions concerning policies, oversight and structures
- Financial decisions concerning budgets, expenditure, investment and assets
- Operational decisions concerning day-to-day management
- Programmer decisions concerning project design and implementation
- Human-resources decisions concerning recruitment, performance and discipline
- Legal and compliance decisions concerning law, contracts and breaches
- Emergency decisions requiring urgent action to protect persons or resources
- The delegation of authority matrix shall identify the competent authority for each class.

Article 18: Decision Memoranda

A decision memorandum setting out shall support every material decision submitted to the competent authority:

- The decision sought
- Brief background
- The matter for determination
- Available options
- Financial and legal analysis
- Risk analysis
- Effects on programs and beneficiaries

- The recommendation
- The person responsible for implementation
- The timetable
- Supporting documents
- A draft resolution.

Article 19: Decision Register

The Organization shall maintain a central register of material decisions recording:

- Decision number and date
- The issuing authority
- The text of the decision
- The implementation owner and deadline
- Implementation status
- Later decisions amending or revoking it
- Confidentiality classification
- Evidence confirming implementation.

Article 20: Implementation and Follow-up of Decisions

Every institutional decision shall be followed by:

- Communication to relevant parties
- Defined implementation actions
- Allocation of required resources
- Assigned responsibilities
- Progress monitoring
- Reporting of delay or obstruction
- Documented completion
- Evaluation of results where appropriate
- A decision is implemented only when the required actions and results have been completed, not merely when it is issued.

Article 21: Reconsideration of Decisions

A previous decision may be reconsidered where material new information emerges, the law changes, financial or operating circumstances change, analysis is shown to be erroneous or deficient, the decision produces an unforeseen or harmful effect, an audit or investigation recommends review, or a material conflict of interest is established. The issuing authority or a higher authority shall undertake reconsideration.

PART V

ACCOUNTABILITY, OVERSIGHT AND INTERNAL CONTROL

Article 22: Accountability Framework

The Organization shall maintain an integrated accountability system under which all authority, decisions, resources and activities are reviewed and evaluated according to the level of responsibility. It includes:

- Accountability of the Board to the General Assembly
- Accountability of the Secretary-General to the Board
- Accountability of Executive Management to the Secretary-General
- Accountability of managers for their staff and teams
- Accountability of committees, programs and projects for results and resources
- Accountability to beneficiaries and affected communities
- Accountability to donors and partners
- Accountability to legal and regulatory authorities
- Accountability for conduct, ethics and safeguarding
- Accountability for programmer results and impact
- Every power shall carry clear responsibility for its use and results.

Article 23: Three Lines Model

The Organization shall apply the Three Lines Model to strengthen risk management, control and assurance:

- First line – operational management: departments, programs, projects and staff identify operational risks, apply controls, comply with policies and procedures, correct errors and breaches, and produce operating reports
- Second line – specialist oversight: risk management, compliance, legal affairs, human resources, finance, safeguarding, security and safety, and data protection functions set standards, advise and monitor first-line compliance
- Third line – independent assurance: Internal Audit or another independent assurance function evaluates the adequacy and effectiveness of governance, risk management and internal control
- The model does not relieve the Board or Executive Management of their primary responsibilities.

Article 24: Internal Control System

The Organization shall establish an effective and proportionate internal control system to:

- Safeguard assets
- Prevent fraud and corruption
- Ensure accurate records

- Support compliance with policies
- Improve operational efficiency
- Ensure proper use of resources
- Protect data and information
- Support reliable reporting
- Reduce errors and losses
- Ensure achievement of institutional objectives
- The system shall include preventive, detective and corrective controls.

Article 25: Management Responsibility for Internal Control

Executive Management has primary responsibility for designing, implementing and monitoring internal controls. Each manager shall:

- Identify risks within the manager's area
- Establish appropriate controls
- Explain procedures to staff
- Monitor compliance
- Remedy deficiencies
- Report material breaches
- Retain evidence and records
- Review controls periodically
- Ensure that controls are not bypassed on grounds of speed or necessity
- Escalate matters beyond delegated authority.

Article 26: Segregation of Duties

So far as practicable, the following duties shall be separated:

- Requesting a transaction
- Approving it
- Executing it
- Recording it
- Receiving goods or services
- Holding assets
- Performing reconciliations
- Reviewing results
- No person shall control all stages of a transaction. Where full separation is impracticable due to limited staffing, compensating controls shall include supervisory review, dual approval, independent reconciliation, post-review, job rotation and surprise checks.

Article 27: Authorization and Approval Controls

No transaction, commitment, expenditure or contract may be executed without approval by the authority designated in the Delegation of Authority Matrix. Approval shall be prior, except in lawful emergencies; written or electronic; issued by an authorized and conflict-free person; based on sufficient information; within prescribed financial and time limits; and verifiable. A transaction shall not be split to avoid an approval threshold.

Article 28: Financial Controls

Financial controls shall include, at a minimum:

- An approved annual budget and clear expenditure limits
- Prior approvals and dual or multiple signatures proportionate to risk
- Monthly bank reconciliations and reconciliation of cash and records
- Review of advances, impress, invoices and supporting documents
- Verification of receipt of goods and services
- Monitoring of budget variances
- Control over electronic transfers, passwords and payment instruments
- Asset counts and periodic financial reports
- Closure of accounts according to an approved timetable.

Article 29: Programmer and Project Controls

Programmers and projects shall be subject to controls including:

- An approved project document, objectives and indicators
- A budget and work plan with assigned responsibilities
- Risk assessment and a procurement plan
- Beneficiary-selection mechanisms and controls against exploitation and favoritism
- Periodic technical and financial reporting
- Monitoring of outputs and outcomes
- Change management and documentation of activities and beneficiaries
- Review of donor-condition compliance
- End-of-project evaluation
- A closure, handover and archiving plan.

Article 30: Control of Branch and Field Offices

Branch and field offices shall be subject to controls ensuring consistency with Organization policies, including written delegated authority, financial and operational limits, regular reporting to headquarters, periodic reviews, asset counts, control of bank accounts and cash, supervisory visits, safeguarding measures, incident and risk reporting, record retention, vetting of staff and volunteers, and office closure or transfer controls. A branch office may not assume a material commitment or alter an Organization policy without approval.

Article 31: Internal Control Self-Assessment

Departments and offices shall periodically assess their internal controls to identify principal risks, existing and unimplemented controls, weaknesses, action owners, deadlines, residual risk and required escalation. Results shall be submitted to Executive Management and the risk and compliance function; material matters shall be presented to the competent Board committee.

PART VI

INTERNAL AND EXTERNAL AUDIT AND ASSURANCE

Article 32: Internal Audit Function

The Organization shall maintain an independent Internal Audit function proportionate to its size and risk profile. A permanent unit, an independent contracted auditor, a specialist external provider, or a shared arrangement with an independent institution may deliver it, provided independence and confidentiality are protected. It shall provide objective assurance on governance, risk management, internal control, financial operations, compliance, asset protection, information systems and programmer and project management.

Article 33: Independence of Internal Audit

Internal Audit shall enjoy organizational and professional independence. It shall report functionally to the Audit, Risk and Compliance Committee and may report administratively to the Secretary-General solely for operational arrangements. Appointment or removal of the Head of Internal Audit requires committee approval. Internal Audit shall have unrestricted access to records, staff and sites, shall not perform operations it audits, shall report interference to the Committee Chairperson, and may meet the Committee without Executive Management.

Article 34: Internal Audit Charter

The Organization shall approve a separate Internal Audit Charter governing purpose, authority, independence, scope, access rights, planning methodology, reporting, recommendation follow-up, confidentiality, professional conduct, quality assurance, coordination with External Audit, and handling suspected fraud.

Article 35: Risk-Based Audit Plan

Internal Audit shall prepare an annual or multi-year risk-based plan considering the enterprise risk register, value of resources, previous audit results, donor requirements, institutional change, sensitive programs, complaints and investigations, financial and technology systems, field offices, fraud and corruption risks, beneficiary safeguarding, and available audit capacity. The Audit, Risk and Compliance Committee shall approve and monitor the plan.

Article 36: Internal Audit Reports

Internal Audit reports shall state the scope, methodology, findings, risk rating of each observation, supporting evidence, impact, root cause, recommendation, management response, implementation owner, deadline and residual risk. Reports shall be accurate, balanced, objective and actionable.

Article 37: Management Response to Audit Findings

Management shall respond to audit findings within the prescribed period. The response shall state acceptance or reasoned disagreement, corrective action, implementation owner, target date,

required resources, and any risk management proposes to accept if the recommendation is not implemented. A finding may be closed only after verification of corrective action.

Article 38: Monitoring Audit Recommendations

The Organization shall maintain a central audit-recommendation register recording the number, source, risk rating, required action, owner, deadline, status, evidence, verification result, closure date, reasons for delay and any risk-acceptance decision. Overdue or high-risk recommendations shall be reported periodically to Executive Management and the Audit, Risk and Compliance Committee.

Article 39: External Audit

The Organization shall appoint an independent and qualified External Auditor in accordance with applicable law, the Constitution and donor requirements. Selection shall consider professional competence, independence, non-profit experience, absence of conflicts, rotation where appropriate, clear scope, confidentiality, report quality, recognized professional standards and disclosure of non-audit services.

Article 40: Relationship with the External Auditor

The Audit, Risk and Compliance Committee shall oversee the External Auditor relationship, including recommending appointment, reviewing independence, approving audit scope, discussing findings, following up the management letter, reviewing fees, meeting privately with the auditor where necessary, evaluating quality, monitoring recommendations and addressing restrictions on the auditor’s work.

Article 41: Other Assurance Activities

The Organization may use additional assurance activities, including donor reviews, compliance assessments, safeguarding assessments, programmer-quality reviews, information-security assessments, human-resources reviews, legal due diligence, partner assessments, procurement-integrity reviews and independent project evaluations. Assurance activities shall be coordinated to avoid duplication and unnecessary burden on resources.

PART VII

COMPLIANCE MONITORING AND REPORTING

Article 42: Compliance Management System

The Organization shall establish a compliance management system to identify and monitor legal, regulatory, and contractual and policy obligations. It shall include an obligations register, assigned responsibilities, monitoring of legal changes, non-compliance risk assessment, training, periodic reviews, reporting of breaches, corrective action, reporting to Management and the Board, and retention of evidence.

Article 43: Compliance Register

The compliance register shall record the legal or regulatory obligation, issuing authority, compliance requirements, internal owner, deadline or frequency, compliance status, required evidence, non-compliance risk, corrective action and date of last review.

Article 44: Compliance Reports

The compliance function shall report periodically to the Secretary-General and the Audit, Risk and Compliance Committee on compliance status, material breaches, overdue obligations, legal developments, assessment results, relevant investigations, corrective action, risk acceptances, training needs and matters requiring decision.

Article 45: Escalation of Material Breaches

The Secretary-General and Chairperson of the Audit, Risk and Compliance Committee shall be notified immediately of any breach capable of causing loss of registration or license, material financial loss, serious harm to beneficiaries, criminal or civil liability, material donor breach, major reputational harm, sensitive data leakage, fraud or corruption, sexual exploitation or abuse, or material programmer disruption. The Board or competent committee shall determine required notification to authorities, donors or partners.

PART VIII

RISK GOVERNANCE AND ENTERPRISE RISK MANAGEMENT

Article 46: Risk Governance Framework

The Organization shall adopt an integrated risk management framework to identify, analyze, treat, monitor and report risks affecting its mission, objectives, resources and beneficiaries. The framework shall:

- Integrate risk management into planning and decisions
- Make every officer responsible for risks within that officer's work
- Priorities beneficiary and staff safety
- Make controls proportionate to risk
- Promote early reporting of emerging risks
- Prohibit concealment of risk to protect reputation or avoid accountability
- Base decisions on reasonable information and evidence
- Review risks regularly
- Document risk-acceptance decisions
- Learn from incidents, errors and losses.

Article 47: Objectives of Enterprise Risk Management

Enterprise risk management seeks to:

- Protect the life, dignity and rights of beneficiaries
- Ensure continuity of essential operations
- Protect assets, funds and data
- Strengthen compliance with law, policy and agreements
- Reduce fraud, corruption and misuse
- Support informed strategic decisions
- Strengthen institutional resilience
- Protect reputation and public confidence
- Improve programmer and project success
- Strengthen financial sustainability
- Support crisis response
- Enable responsible pursuit of opportunities.

Article 48: Risk Categories

Institutional risks include strategic, financial, operational, legal and regulatory, governance, fraud and corruption, safeguarding, programmer and project, human resources, security and safety, information and cyber-security, reputational, partner and third party, funding and donor, environmental and climate, public health and epidemic, conflict and political-disruption, business-continuity, supply-chain and procurement, and beneficiary legal-protection risks.

Article 49: Risk Appetite

The Board shall approve a risk-appetite statement defining the overall risk the Organization is prepared to accept in pursuing its objectives. It shall address beneficiary safety, safeguarding, legal compliance, fraud and corruption, security and safety, finance, innovation and new programs, partnerships, technology and data, reputation, funding and sustainability, and work in high-risk environments. Appetite for exploitation, abuse, intentional fraud, serious corruption and deliberate harm to beneficiaries shall be extremely low or zero.

Article 50: Risk-Tolerance Limits

Executive Management, with approval of the Board or competent committee, shall establish quantitative or qualitative tolerance limits for material risks. These may cover acceptable financial loss, project delay, budget variance, system or service downtime, overdue legal obligations, staff turnover, security incidents, donor concentration, partner exposure and unresolved high-risk findings. Any breach shall be escalated immediately.

Article 51: Risk Identification

Risks shall be identified regularly through strategic planning, programmer and project design, departmental assessments, analysis of the political and legal environment, incident and complaint reports, audit results, partner and supplier assessments, beneficiary consultations, data and indicator analysis, management and committee meetings, lessons from previous projects, technology, environmental and economic developments, security assessments, and review of donor and contract terms. Identification shall also include opportunities that may advance the mission.

Article 52: Risk Assessment

Risks shall be assessed by likelihood and impact, considering effects on persons, finance, law, programs, reputation and data; speed and duration; detectability; effectiveness of existing controls; interdependence with other risks; and residual risk. Approved categories shall include low, medium, high and critical.

Article 53: Risk Ownership

A competent owner with authority to influence causes and controls shall be assigned to each material risk. The owner shall monitor and update the risk, implement treatment, collect evidence, report changes, request resources, escalate breaches of tolerance, coordinate with relevant functions, monitor early-warning indicators and report periodically. Internal Audit shall not own risks it audits.

Article 54: Risk Treatment

Risks may be avoided, reduced, transferred through lawful insurance or contracting, shared, formally accepted, or—where linked to a legitimate benefit—used to pursue an opportunity. A treatment plan shall specify the action, owner, resources, deadline, indicator, expected residual risk and verification method.

Article 55: Risk Acceptance

A material risk shall not be accepted implicitly or without documentation. The decision shall describe the risk, reasons, existing controls, residual level, potential consequences, acceptance period, monitoring owner, reassessment triggers, approving authority and consistency with risk appetite. No risk may be accepted where it violates law or exposes beneficiaries to serious unjustified harm.

Article 56: Enterprise Risk Register

The Organization shall maintain a central enterprise risk register containing the risk number, description, category, causes, potential consequences, likelihood, impact, overall rating, controls, control-effectiveness assessment, residual risk, owner, treatment plan, deadline, early-warning indicators, implementation status, last review, escalation body, any acceptance decision and linkage to organizational objectives.

Article 57: Departmental and Project Risk Registers

Every department, office, programmer and project shall maintain a proportionate risk register linked to the enterprise register. Registers shall be updated regularly, reviewed in management meetings, escalate high and critical risks, link risks to work plans and budgets, identify owners, document treatment, be reviewed upon material change, include partner, supplier, safeguarding and data risks, and close risks only after verified treatment.

Article 58: Risk Escalation

A risk shall be escalated where it exceeds appetite or tolerance, is beyond the owner's authority, requires material additional resources, affects several functions, may harm beneficiaries or staff, may cause material loss or legal or contractual breach, may damage reputation, is subject to ineffective controls, or requires a Board or committee decision. Escalation shall be documented and state the risk, recommendation and decision sought.

Article 59: Key Risk Indicators

The Organization shall establish key risk indicators to identify increasing exposure before harm occurs. Indicators may include falling liquidity, budget variances, increasing complaints, repeated security incidents, delayed donor reports, staff turnover, weak attendance or performance, increasing control findings, funding concentration, system outages, data-protection incidents, procurement breaches, delayed corrective action and changes in the legal or political environment. Warning thresholds shall trigger alert or escalation.

Article 60: Risk Reports

Executive Management shall report periodically to the Board or Audit, Risk and Compliance Committee on principal enterprise risks, changes since the previous report, new and emerging risks, tolerance breaches, treatment status, overdue actions, material incidents, control effectiveness, risk acceptances, required resources, possible scenarios and decisions required from the Board.

Article 61: Scenario Analysis and Stress Testing

Where appropriate, the Organization shall conduct scenario analysis and stress testing for major events such as loss of a principal donor, frozen bank accounts, closure of an office or programmer, armed conflict or civil unrest, cyber intrusion, data loss, epidemic or public-health emergency, serious safeguarding allegation, sudden departure of key leaders, a sharp rise in beneficiary numbers, supply-chain disruption, or a reputational or media crisis. Results shall inform contingency plans, budgets and continuity strategies.

Article 62: Project Risk Assessment

No material project shall be approved without a proportionate assessment of mission alignment, actual beneficiary needs, security, safeguarding, financial, partner, procurement, legal and reputational risks, operating capacity, donor requirements, sustainability and exit planning, effects on host communities, environmental and climate risks, and beneficiary-selection controls.

Article 63: Partner and Third-Party Risks

Before a material partnership or contract, the Organization shall assess the third party's legal status, reputation, technical experience and capacity, financial stability, control systems, safeguarding record, conflicts of interest, anti-fraud and anti-corruption commitment, data security, sanctions and legal restrictions, political affiliations or undisclosed interests, delivery capacity, complaints system and previous assessments or reviews. Due-diligence depth shall be proportionate to risk.

Article 64: Security Risk Management

The Organization shall maintain a security risk management system protecting beneficiaries, staff, volunteers, assets and information. It shall include site assessments, security and safety plans, travel and movement procedures, evacuation plans, incident reporting, emergency communications, staff training, visitor management, and office and event security, protection for work in high-risk environments, threat analysis and review of insurance arrangements where appropriate.

Article 65: Risk Review and Continuous Improvement

The risk management framework shall be reviewed periodically for suitability and effectiveness. Review shall address the quality of risk registers, effectiveness of treatment, accuracy of likelihood and impact ratings, owner performance, escalation, unforeseen and recurring incidents, audit results, donor and partner observations, crisis lessons, adequacy of resources, and any need to amend appetite or tolerance. Material improvements require Board approval.

PART IX

ACCOUNTABILITY TO AFFECTED POPULATIONS AND STAKEHOLDER ENGAGEMENT

Article 66: Accountability to Affected Populations

The Organization is genuinely accountable to beneficiaries, refugees and host communities and shall ensure their right to clear information on programs and services, eligibility and selection criteria, participation in activity design, expression of views without fear, confidential and safe complaints, appropriate response, protection from retaliation, knowledge of service limitations, participation in evaluation, and services free from exploitation or discrimination.

Article 67: Stakeholder Identification

For every programmer or material decision, the Organization shall identify stakeholders and analyze their relationship to the Organization, degree of impact, ability to influence, information needs, exclusion risks, engagement methods, access and language needs, participation-related safeguarding risks, potential conflicts of interest and priority for consultation.

Article 68: Inclusive Participation

Participation shall be inclusive, safe and respectful of diversity, with particular attention to women and girls, children and youth, persons with disabilities, older persons, minorities, survivors of violence or torture, persons with special legal or protection needs, persons facing language or digital barriers, host communities and hard-to-reach groups. Participation shall not expose identity or place any person at risk.

Article 69: Information Provided to Beneficiaries

Beneficiaries shall receive timely, accurate and understandable information on the programmer, available services, eligibility criteria, duration, responsibilities of the Organization and beneficiary, complaint channels, codes of conduct, protection from exploitation and abuse, use of personal data, limits of confidentiality, partners and any service changes. Information shall be provided in a language and format suited to the target group.

Article 70: Complaints and Feedback Mechanisms

The Organization shall maintain multiple safe and accessible channels for beneficiaries, staff, volunteers, partners and community members, which may include complaint boxes, telephone and helplines, email, online forms, in-person interviews, community focal points, beneficiary representatives, partner referrals, separate sensitive-complaint channels and formats adapted to disability, language, age and gender. Channels shall be free, confidential and clearly publicized.

Article 71: Principles for Handling Complaints

Complaints shall be handled with respect and dignity, confidentiality, impartiality and independence, reasonable promptness, non-discrimination, protection of complainants and witnesses, non-retaliation, survivor-centered and child-sensitive safeguards, the right of

response, documented procedures, data protection and safe referral. A complaint shall not be rejected merely because it is oral or the complainant is unfamiliar with formal procedure.

Article 72: Classification of Complaints

Complaints shall be classified by nature and severity, including inquiries, service-quality observations, delay or mistreatment, discrimination or favoritism, eligibility disputes, staff or volunteer misconduct, fraud and corruption, conflicts of interest, misuse of data, harassment or bullying, sexual exploitation and abuse, child abuse, security risks and serious legal breaches. Response, investigation and escalation shall be proportionate to severity.

Article 73: Receipt and Acknowledgement of Complaints

Upon receipt, a complaint shall be assigned a reference number; its date, channel and nature shall be recorded; urgency and immediate protection needs assessed; receipt acknowledged where safe and possible; expected steps explained; the handling authority identified; identity protected; and unnecessary information avoided.

Article 74: Complaint-Handling Timeframes

The Organization shall adopt reasonable timeframes proportionate to the nature, complexity and severity of complaints. Simple inquiries shall be addressed promptly; immediate action shall be taken where a person is at risk; material delay shall be communicated; investigative quality shall not be sacrificed for speed; overdue matters shall be reviewed and unjustified delay escalated; and extensions shall be documented.

Article 75: Investigation of Complaints

Complaints requiring investigation shall be handled under written procedures defining scope, appointing a qualified and impartial investigator, avoiding conflicts, preserving evidence, interviewing relevant parties, protecting survivors and witnesses, respecting the presumption of innocence, documenting findings, applying the approved standard of proof, making actionable recommendations, referring to authorities where required and avoiding interference with official investigations.

Article 76: Communication of Complaint Outcomes

Where lawful, safe and appropriate, the complainant shall be informed of the outcome in a manner that preserves confidentiality and data protection, protects the respondent’s rights and witness safety, does not reveal sensitive investigative information, indicates whether action was taken, explains review or appeal rights and identifies available support or referral.

Article 77: Grievance and Review of Decisions

A complainant or affected person may request review where new evidence emerges, a material procedural breach occurred, a conflict of interest existed, the outcome is not reasonably supported by evidence, the sanction is manifestly disproportionate, or safeguarding risks were not considered. Review shall be undertaken by a person or body not involved in the original decision.

Article 78: Protection from Retaliation

Retaliation is prohibited against a complainant, whistleblower, witness, survivor, information provider, person refusing to participate in misconduct, or person cooperating with an investigation or review. Retaliation includes dismissal, threats, bullying, reduction of responsibilities, and denial of services, defamation or any other adverse action.

Article 79: Whistleblowing Mechanism

The Organization shall maintain an independent and safe mechanism for reporting serious wrongdoing, including fraud, corruption and bribery, misuse of resources, legal breaches, undisclosed conflicts, concealment of misconduct, safeguarding violations, falsification of records, abuse of authority and retaliation. Reports may be identified or anonymous, subject to the Organization's ability to verify the information.

Article 80: Complaints and Reports Register

A secure, access-restricted register shall record the reference number, receipt date, classification, severity, handling authority, actions, investigation status, preventive measures, outcome, closure date, recommendations, corrective-action status, any report to competent authorities and retention period. General registers shall not include identifying details except where necessary.

Article 81: Complaints Reporting and Institutional Learning

Periodic anonymized reports to Executive Management and the Board shall cover complaint volume and types, channels, handling times, overdue matters, recurring trends, institutional risks, corrective actions, safeguarding complaints, measurable complainant satisfaction, service-improvement recommendations and matters requiring policy or procedural change. Statistical reporting shall not identify individuals or small communities.

Article 82: Beneficiary Participation in Monitoring and Evaluation

Beneficiaries shall be involved appropriately and voluntarily in programmer monitoring and evaluation through surveys, focus groups, interviews, community committees, participatory assessments, learning and review sessions, community validation of results, inclusion of persons with disabilities and marginalized groups, post-project feedback and accessible dissemination of evaluation results. Participation shall be safe and shall not affect entitlement to services.

PART X

TRANSPARENCY, DISCLOSURE AND ACCESS TO INFORMATION

Article 83: Commitment to Transparency

The Organization shall be transparent in its operations, decisions and use of resources, subject to lawful restrictions relating to confidentiality, data protection and security. Transparency includes clarity of structure and authority, appropriate reporting, disclosure of material funding sources, beneficiary-selection criteria and complaint channels, lawful conflict disclosure, explanation of material decision processes, access to core public policies and correction of inaccurate information.

Article 84: Public Information

The Organization may publish through its official website, reports or approved media its legal name and registration, mission, vision and values, organizational structure, Board and senior leadership where lawful, programs and geographic areas, annual report, audited financial statements or summary, principal partners and donors, core public policies, contact and complaint channels, achievements and indicators, and employment, volunteering and contracting opportunities.

Article 85: Confidential and Restricted Information

Information shall be confidential or restricted where disclosure may endanger a person, violate beneficiary or staff privacy, prejudice an investigation, breach a legal or contractual obligation, reveal security information, prejudice a legal position, disclose legitimate trade secrets, compromise competitive procurement, identify a whistleblower or witness, or endanger information systems. Classification shall not be used to conceal wrongdoing or avoid lawful accountability.

Article 86: Requests for Information

Stakeholders may request non-confidential institutional information. Requests shall be recorded, assigned to a responsible function, reviewed for legal restrictions, answered within a reasonable time and, where practicable, in an accessible format. Any refusal or partial withholding shall be explained and may be internally reviewed, while personal data shall be protected.

Article 87: Approval of Publications

Material institutional information shall be published only after review and approval by the authorized body, verifying accuracy, completeness, consistency with institutional positions, intellectual-property rights, data protection, safety, donor conditions and appropriate language and style. An approved final copy shall be retained and the spokesperson or follow-up owner identified.

PART XI

GOVERNANCE OF PARTNERSHIPS AND THIRD PARTIES

Article 88: Partnership Principles

Partnerships shall be based on mission alignment, mutual respect, clear roles, transparency, accountability, non-discrimination, beneficiary safeguarding, financial integrity, fair risk sharing, local capacity strengthening, respect for each party's independence and clear benefit.

Article 89: Partner Selection

Partners shall be selected objectively based on legal status, values alignment, reputation, technical experience, financial and administrative capacity, safeguarding record, control systems, beneficiary access, independence and absence of conflicts, reporting capacity, anti-fraud and anti-corruption commitment and data-protection capacity. Selection reasons shall be documented.

Article 90: Partner Due Diligence

Before approval, risk-based due diligence shall review registration documents, constitution, management structure, leadership, financial statements, bank accounts, references, key policies, litigation or breach history, sanctions or legal restrictions, conflicts of interest, field visits, safeguarding and security assessments and operating capacity.

Article 91: Partnership Agreements

Every material partnership shall be documented by a written agreement stating purpose and scope, term, roles, outputs and indicators, budget and funding, disbursement and reporting, procurement and assets, safeguarding, data protection, intellectual property, confidentiality, audit and record access, complaints, dispute resolution, suspension and termination, recovery of funds and assets, governing law and post-termination obligations.

Article 92: Partner Monitoring

Partners shall be monitored through technical and financial reports, document review, field visits, verification of activities and beneficiaries, procurement review, complaints follow-up, safeguarding compliance, indicator review, audits where needed, updated risk assessments, monitoring meetings and improvement plans. Monitoring intensity shall increase with risk.

Article 93: Partner Non-Compliance

For partner non-compliance, proportionate measures may include requesting clarification, a corrective plan, training or technical support, and enhanced oversight, suspension of a payment or activity, recovery of funds, donor notification, termination, and referral to authorities, and exclusion from future partnerships and protection of affected beneficiaries.

PART XII

DATA, INFORMATION AND DIGITAL SYSTEMS GOVERNANCE

Article 94: Data Governance Principles

Data shall be managed according to lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality and security, accountability, respect for data-subject rights, do no harm, protection of vulnerable-group data and responsible use of technology.

Article 95: Data Ownership and Stewardship

Data collected or created through the Organization's work is an institutional resource subject to control and protection. The Organization shall designate a data owner responsible for purpose and accountability, a steward for daily management, authorized users on a need basis, a systems-security owner and, where appropriate, a data-protection officer. No staff member or member may treat institutional data as personal property.

Article 96: Lawful Collection and Consent

Personal data shall be collected only for a specific lawful purpose and to the extent necessary. Where appropriate, the Organization shall explain the purpose, use, recipients, retention period and limits of confidentiality; obtain free and informed consent; consider parental consent and the best interests of the child; permit withdrawal where lawful; provide alternatives where consent is not possible; and document the lawful basis for processing.

Article 97: Data Access Controls

Access shall be based on need to know and least privilege. Controls shall include individual user accounts, strong passwords, and multi-factor authentication where possible, periodic access review, removal upon separation, encryption of sensitive data, access logs, segregation of highly sensitive data, prohibition on password sharing and prior approval for data transfer.

Article 98: Data Sharing

Data shall be shared with a third party only for a lawful and necessary purpose, with an appropriate lawful basis or consent, risk assessment, a data-sharing agreement where needed, defined recipient duties, adequate security, data minimization, enhanced protection for children and survivors, and the ability to stop sharing in the event of misuse.

Article 99: Data Retention and Disposal

The Organization shall adopt a retention schedule specifying record type, period, legal or contractual basis, storage location, protection level, record owner, destruction method and any legal hold arising from investigation or dispute. Disposal shall securely prevent recovery or misuse.

Article 100: Data Breach Management

A suspected data breach shall be contained immediately; affected systems protected; evidence preserved; data types and affected persons assessed; potential harm evaluated; the competent officer notified; authorities or individuals informed where required; support provided; the incident documented; root cause identified; corrective action implemented; and controls and training reviewed.

Article 101: Cyber-Security Governance

Cyber-security controls shall include system updates, anti-malware protection, backups, device control, email protection, phishing awareness, vulnerability management, incident response, remote-access protection, technology-vendor review, restoration testing and protection of official websites and platforms.

Article 102: Artificial Intelligence and Automated Tools

Artificial-intelligence tools shall be used responsibly and ethically. Personal or confidential data shall not be entered into unapproved tools; outputs shall be human-reviewed and checked for accuracy and bias; high-impact decisions shall not be automated without human oversight; intellectual property shall be respected; use shall be disclosed where appropriate; children and vulnerable groups protected; legal and security risks assessed; human accountability retained; and tools approved by the competent technology function.

PART XIII

PERFORMANCE MANAGEMENT, MONITORING, EVALUATION AND LEARNING

Article 103: Institutional Performance Framework

The Organization shall maintain an integrated performance framework linking the vision and mission, strategic plan, annual plans, budgets, programs and projects, performance indicators, individual responsibilities, results reports, risk management, learning and improvement.

Article 104: Key Performance Indicators

Performance indicators shall be linked to objectives, clearly defined, measurable and verifiable, supported by an identified source, owner and frequency, disaggregated by sex, age and disability where appropriate, balanced between quantity and quality, and focused on outcomes and impact as well as activities.

Article 105: Monitoring System

The monitoring system shall ensure timely data collection, data-quality verification, comparison of results against plan, identification of delay and variance, corrective action, risk monitoring, beneficiary participation, evidence documentation, dashboards and escalation of material issues to Management and the Board.

Article 106: Evaluations

Subject to need and resources, evaluations may include baseline, mid-term, final, impact, independent, participatory, rapid emergency, thematic or sectoral, partnership and sustainability evaluations. They shall be objective, evidence-based, ethical and safeguarding-sensitive.

Article 107: Data Quality Assurance

Performance data shall be assessed for accuracy, completeness, consistency, timeliness, reliability, integrity, traceability and protection. Periodic data reviews shall be conducted, and results shall not be altered or inflated to satisfy donors or Management.

Article 108: Performance Reports

Performance reports shall present achieved results, comparison against targets, analysis of variances, challenges, risks, resource use, beneficiary feedback, lessons learned, corrective action, decisions required, and identity-protected stories of change, sustainability and next steps.

Article 109: Learning and Knowledge Management

The Organization shall preserve and share knowledge through after-action reviews, lessons-learned meetings, document repositories, and practice guides, communities of learning, and knowledge transfer during staff changes, documentation of innovation, sharing results with partners, experience-based policy updates and protection of sensitive knowledge.

PART XIV

GOVERNANCE REVIEW, EFFECTIVENESS AND FINAL PROVISIONS

Article 110: Annual Governance Review

An annual governance review shall assess whether governing bodies act within mandate, Board and committee effectiveness, decision implementation, report quality, risk management, compliance, conflicts of interest, partner performance, complaint mechanisms, beneficiary safeguarding, deficiencies and corrective action.

Article 111: Independent Governance Evaluation

The Board may commission an independent governance evaluation, particularly following substantial institutional growth, geographic expansion, leadership change, repeated breaches, donor requirements, merger or restructuring, a crisis, or a prolonged period without independent evaluation.

Article 112: Governance Improvement Plan

Where deficiencies are identified, the Organization shall approve an improvement plan specifying the deficiency, risk level, corrective action, owner, resources, deadline, indicator, verification method, monitoring body and implementation status.

Article 113: Relationship with Other Policies

These Regulations shall be read together with the Constitution, Board of Directors Rules of Procedure, Financial Regulations, Procurement Policy, Human Resources Regulations, Code of Conduct, Conflict of Interest Policy, Anti-Fraud, Anti-Corruption and Anti-Bribery Policy, Safeguarding Policy, Complaints Policy, Data Protection Policy, Risk Management Policy, Internal Audit Charter, committee terms and programmer and project policies. In case of conflict, precedence is: applicable law; the Constitution; General Assembly resolutions; the Board Rules and these Regulations according to their respective subject matter; then executive policies and procedures.

Article 114: Interpretation

These Regulations shall be interpreted consistently with applicable law, the Constitution, the Organization’s mission, beneficiary safeguarding, integrity and accountability, good-governance principles, institutional sustainability and lawful donor and partner requirements. The Legal Adviser, together with the Strategy and Governance Department, shall provide a written opinion; the Board shall adopt interpretations within its mandate; and the General Assembly has final authority where its powers or a possible conflict with the Constitution are concerned.

Article 115: Exceptions

An exception may be granted only for a legitimate documented reason, following risk assessment, by an authorized body, for a defined period, without violating law or the Constitution, with compensating controls and notification to the competent oversight body where

material. No exception may permit fraud, corruption, exploitation, data misuse or harm to beneficiaries.

Article 116: Breach of these Regulations

A breach may result in corrective, disciplinary or contractual action, including direction, training, warning, reversal of an unlawful decision, recovery of funds or assets, withdrawal of authority, investigation, and disciplinary sanction, termination of a contract or partnership, referral to authorities, remedy for harm to beneficiaries and modification of the control system.

Article 117: Review Cycle

These Regulations shall be reviewed at least every three years, or earlier following amendment of the Constitution, changes in law or organizational structure, emerging risks, audit or evaluation findings, donor or regulatory requirements, an institutional crisis, or expansion of programs or geographic operations.

Article 118: Amendment

These Regulations may be amended on the recommendation of the Board and approval of the General Assembly, subject to the approval authority and any special majority prescribed by the Constitution. Reasons shall be documented, legal review completed, the draft circulated before approval, the effective date and version number recorded, affected persons notified and obsolete copies withdrawn.

Article 119: Entry into Force

These Regulations enter into force upon approval by the General Assembly and bind all members, leaders, staff, volunteers, partners and contractors to the extent applicable. Previous provisions inconsistent with them are repealed. The General Assembly approved these Regulations at its meeting held on 15 August 2026 and authorized the Board Chairperson and Legal Adviser to sign on behalf of the members and affix the Organization's seal.

ADOPTION AND APPROVAL

1. Adopted by the General Assembly at its meeting held on 31 December 2025.
2. The General Assembly authorizes the Board Chairperson and Legal Adviser to sign on behalf of all members and the Organization's official seal shall be affixed.

Signature of the Board Chairperson: **Signature of the Legal Adviser:**