ANTI-FRAUD, CORRUPTION AND WHISTLEBLOWING POLICY

FOR THE

INITIATIVE FOR LEGAL AID

(ILA)

ANTI-FRAUD, CORRUPTION AND WHISTLEBLOWING POLICY

INITIATIVE FOR LEGAL AID (ILA)

TABLE OF CONTENTS

CHAPTER SIX: **PROHIBITED CONDUCT**

6.1 Fraud
6.2 Corruption
6.3 Bribery
6.4 Theft
6.5 Misappropriation
6.6 Procurement Fraud
6.7 Payroll Fraud
6.8 Grant Fraud
6.9 Asset Theft
6.10 Abuse of Authority
6.11 Manipulation of Records
6.12 Bid Rigging
6.13 False Reporting
6.14 Programme Fraud
6.15 Cyber Fraud
6.16 Obstruction of Investigations
6.17 Retaliation

CHAPTER SEVEN: **CONFLICT OF INTEREST MANAGEMENT**

7.1 Policy Principles
7.2 Disclosure Requirements
7.3 Register of Interests
7.4 Gifts and Hospitality
7.5 Related Party Transactions
7.6 Outside Employment
7.7 Political Activities
7.8 Family Relationships
7.9 Procurement Conflicts
7.10 Management Measures

CHAPTER EIGHT: **GIFTS, HOSPITALITY, DONATIONS AND SPONSORSHIPS**

8.1 Acceptable Gifts
8.2 Prohibited Gifts
8.3 Gift Register
8.4 Hospitality
8.5 Travel Sponsorship
8.6 Donations
8.7 Charitable Contributions
8.8 Political Contributions
8.9 Approval Procedures

CHAPTER NINE: **WHISTLEBLOWING FRAMEWORK**

9.1 Principles
9.2 Protected Disclosures
9.3 Anonymous Reporting
9.4 Confidential Reporting
9.5 Reporting Channels
9.6 Hotline
9.7 Email
9.8 Complaint Boxes
9.9 External Reporting
9.10 Emergency Reporting

CHAPTER TEN: **WHISTLEBLOWER PROTECTION**

10.1 Confidentiality
10.2 Protection Against Retaliation
10.3 Witness Protection
10.4 Protection of Evidence
10.5 Psychological Support
10.6 Remedies
10.7 False Reports
10.8 Good Faith Reports

CHAPTER ELEVEN: **INVESTIGATION MANAGEMENT**

11.1 Investigation Principles
11.2 Case Assessment
11.3 Investigation Planning
11.4 Collection of Evidence
11.5 Digital Evidence
11.6 Interviews
11.7 Investigation Reports
11.8 Investigation Standards
11.9 Quality Assurance
11.10 Case Closure

CHAPTER TWELVE: **DISCIPLINARY, ADMINISTRATIVE AND LEGAL ACTION**

12.1 Disciplinary Measures
12.2 Administrative Measures
12.3 Contractual Remedies
12.4 Civil Recovery
12.5 Criminal Referral
12.6 Recovery of Assets
12.7 Debarment

CHAPTER SEVENTEEN: **MONITORING, COMPLIANCE, AUDIT AND REPORTING**

17.1 Compliance Monitoring
17.2 Internal Audit
17.3 External Audit
17.4 Compliance Reviews
17.5 Fraud Indicators
17.6 Annual Reports
17.7 Key Performance Indicators

CHAPTER EIGHTEEN: **ROLES, RESPONSIBILITIES AND ACCOUNTABILITY**

18.1 Board
18.2 Executive Director
18.3 Senior Management
18.4 Finance
18.5 Procurement
18.6 Human Resources
18.7 ICT
18.8 MEAL
18.9 Programme Staff
18.10 Volunteers
18.11 Consultants
18.12 Partners
18.13 Suppliers

CHAPTER NINETEEN: **POLICY IMPLEMENTATION**

19.1 Implementation Strategy
19.2 Action Plans
19.3 Institutional Responsibilities
19.4 Resource Allocation
19.5 Compliance Framework
19.6 Reporting

CHAPTER TWENTY: **POLICY REVIEW, AMENDMENT AND APPROVAL**

20.1 Policy Review
20.2 Amendment Procedure
20.3 Version Control
20.4 Approval
20.5 Transitional Arrangements
20.6 Effective Date

ANNEXES

Annex I – Fraud Risk Assessment Matrix
Annex II – Fraud Risk Register Template
Annex III – Conflict of Interest Declaration Form
Annex IV – Annual Conflict of Interest Disclosure Form
Annex V – Whistleblower Reporting Form
Annex VI – Anonymous Complaint Form
Annex VII – Investigation Terms of Reference Template
Annex VIII – Investigation Report Template
Annex IX – Evidence Collection and Chain of Custody Form
Annex X – Interview Record Form
Annex XI – Gifts and Hospitality Register
Annex XII – Fraud Incident Register
Annex XIII – Corrective Action Tracking Form
Annex XIV – Fraud Response Checklist
Annex XV – Anti-Fraud Due Diligence Checklist for Partners and Suppliers
Annex XVI – Declaration of Compliance with the Anti-Fraud, Corruption and Whistleblowing Policy

CHAPTER ONE

INTRODUCTION, POLICY FRAMEWORK AND GOVERNING PRINCIPLES

1.1 Introduction

The Initiative for Legal Aid (ILA) is committed to conducting all its operations with the highest standards of integrity, transparency, accountability, professionalism and ethical conduct. As a non-governmental, non-profit organization dedicated to advancing access to justice, human rights, legal empowerment and the rule of law in the Republic of South Sudan, ILA recognizes that public confidence, donor trust and institutional credibility are among its most valuable assets.

Fraud, corruption, bribery, theft, embezzlement, abuse of authority and other forms of misconduct undermine organizational effectiveness, divert resources intended for beneficiaries, weaken governance systems, expose the organization to financial and legal risks, and damage relationships with donors, government institutions, partners and the communities that ILA serves. Such misconduct is incompatible with ILA's core values and shall not be tolerated under any circumstances.

ILA acknowledges that fraud and corruption can occur in any organization regardless of its size, governance structure or internal controls. Risks may arise during programme implementation, financial management, procurement, recruitment, partnership management, grant administration, asset management, information technology, monitoring and evaluation, or through interactions with external stakeholders. Consequently, preventing and responding to fraud and corruption requires a comprehensive institutional approach that combines strong governance, effective internal controls, ethical leadership, staff awareness, robust reporting mechanisms and continuous monitoring.

This Anti-Fraud, Corruption and Whistleblowing Policy establishes the framework through which ILA shall prevent, detect, report, investigate and respond to actual or suspected fraud, corruption and related misconduct. It also establishes mechanisms for protecting individuals who report concerns in good faith and promotes a culture in which integrity and accountability are shared responsibilities across the organization.

The Policy applies equally to members of the Board of Directors, management, employees, interns, volunteers, consultants, contractors, suppliers, implementing partners, sub-grantees and any other persons acting for or on behalf of ILA. Every person associated with the organization has an obligation to uphold the principles contained in this Policy and to contribute to safeguarding organizational resources and reputation.

1.2 Background

The operating environment within which ILA delivers legal aid and human rights programmes presents a range of financial, operational, governance and compliance risks. The organization manages donor funds, public resources, confidential information, legal case records, procurement

processes and partnerships with national and international stakeholders. These activities require strong accountability mechanisms to ensure that resources are used solely for their intended purposes.

International experience demonstrates that organizations working in humanitarian, development and human rights sectors are exposed to various forms of fraud and corruption, including procurement fraud, payroll fraud, grant fraud, falsification of programme records, diversion of beneficiary assistance, conflicts of interest, cyber fraud and abuse of authority. Such risks may arise from internal weaknesses, external pressures, inadequate oversight or deliberate criminal conduct.

ILA recognizes that fraud prevention is considerably more effective and less costly than responding to fraud after it has occurred. Accordingly, this Policy emphasizes prevention through effective governance, risk management, internal controls, ethical leadership, segregation of duties, transparency and continuous capacity development.

The organization further recognizes that effective whistleblowing systems are essential components of institutional accountability. Persons who report concerns often provide the earliest indication of fraud or misconduct and therefore play a critical role in protecting organizational resources. ILA is committed to creating a safe environment in which concerns may be reported without fear of retaliation or victimization.

This Policy therefore complements ILA's broader governance framework by integrating fraud prevention into organizational planning, financial management, procurement, human resource management, monitoring and evaluation, information management and risk management systems.

1.3 Policy Statement

The Initiative for Legal Aid adopts a strict zero-tolerance approach to fraud, corruption, bribery, theft, embezzlement, money laundering, facilitation payments, abuse of authority, conflicts of interest, unethical conduct and all other forms of dishonesty.

ILA shall not knowingly permit, condone, ignore or conceal any fraudulent or corrupt practice committed by persons associated with the organization, irrespective of their position, authority, contractual status or length of service.

To uphold this commitment, ILA shall:

a) establish and maintain effective systems of governance, internal control and risk management designed to prevent fraud and corruption;

b) promote an organizational culture founded on integrity, accountability, transparency, professionalism and ethical leadership;

c) ensure that all allegations of fraud, corruption and misconduct are reported, assessed, investigated and resolved promptly, fairly and confidentially;

d) protect whistleblowers and all persons participating in investigations from retaliation, intimidation or victimization;

e) apply appropriate disciplinary, contractual, administrative and legal measures against individuals responsible for misconduct;

f) recover organizational assets and financial losses wherever legally and practically possible;

g) cooperate with competent government authorities, donors and law enforcement agencies where criminal conduct or contractual obligations require disclosure or legal action;

h) continuously strengthen institutional systems through learning, audits, risk assessments, monitoring and periodic policy review.

1.4 Purpose of the Policy

The purpose of this Policy is to establish a comprehensive institutional framework for preventing, detecting, reporting, investigating and responding to fraud, corruption, bribery and related misconduct within Initiative for Legal Aid.

Specifically, this Policy seeks to:

a) safeguard donor funds, grants, organizational assets and financial resources;

b) protect beneficiaries, communities and stakeholders from misconduct affecting programme implementation;

c) strengthen institutional governance, accountability and ethical conduct;

d) establish clear reporting and whistleblowing mechanisms;

e) ensure fair, objective and timely investigations into suspected misconduct;

f) protect individuals who report concerns in good faith;

g) establish clear responsibilities for all persons associated with ILA;

h) strengthen compliance with applicable laws, donor agreements and international standards;

i) promote public confidence in the integrity and credibility of ILA.

1.5 Policy Objectives

The objectives of this Policy are to:

a) establish an organization-wide framework for fraud risk management;

b) define prohibited conduct and unacceptable practices;

c) promote ethical leadership and responsible stewardship of organizational resources;

d) strengthen internal control systems across all organizational functions;

e) enhance transparency in financial management, procurement and programme implementation;

f) encourage early detection and reporting of suspected misconduct;

g) provide accessible, confidential and secure whistleblowing mechanisms;

h) ensure that allegations are investigated professionally, independently and impartially;

i) facilitate recovery of assets and losses resulting from fraud or corruption;

j) strengthen compliance with donor requirements, contractual obligations and legal standards;

k) foster continuous learning and institutional improvement based on investigation outcomes and audit findings.

1.6 Scope of the Policy

This Policy applies to all governance, administrative, operational, financial and programme activities undertaken by or on behalf of ILA, regardless of funding source, project location or contractual arrangement.

It applies to:

a) members of the Board of Directors;

b) the Executive Director;

c) senior management;

d) all permanent, temporary and casual employees;

e) interns and volunteers;

f) consultants and technical advisers;

g) contractors and suppliers;

h) implementing partners and sub-grantees;

i) members of committees and advisory bodies;

j) any individual or entity acting for or representing ILA.

The Policy applies throughout the lifecycle of organizational activities, including planning, budgeting, procurement, recruitment, programme implementation, financial management, monitoring and evaluation, reporting, grant management, information management and asset disposal.

It further applies to all organizational resources, including financial assets, donor funds, grants, equipment, vehicles, information systems, intellectual property, confidential information, digital records and any other property owned, leased or managed by ILA.

1.7 Guiding Principles

Implementation of this Policy shall be guided by the following principles:

1.7.1 Integrity: All persons associated with ILA shall perform their responsibilities honestly, ethically and in the best interests of the organization and its beneficiaries.

1.7.2 Transparency: Organizational decisions, financial transactions, procurement processes and programme activities shall be conducted openly and supported by accurate documentation.

1.7.3 Accountability: Every individual entrusted with authority, resources or responsibilities shall be accountable for their actions and decisions.

1.7.4 Fairness: Allegations of misconduct shall be assessed and investigated objectively, without bias, discrimination or improper influence.

1.7.5 Confidentiality: Information relating to reports, whistleblowers, investigations and disciplinary processes shall be protected and disclosed only to authorized persons with a legitimate need to know.

1.7.6 Non-Retaliation: ILA shall protect whistleblowers, witnesses and other persons participating in accountability processes from retaliation, intimidation, harassment or victimization.

1.7.7 Due Process: Persons accused of misconduct shall be treated fairly, afforded an opportunity to respond to allegations and subject to decisions based on credible evidence.

1.7.8 Continuous Improvement: ILA shall continually strengthen its fraud prevention framework through audits, monitoring, investigations, risk assessments, training and lessons learned.

1.8 Legal and Regulatory Framework

This Policy is developed in accordance with the Constitution and applicable laws of the Republic of South Sudan, internationally recognized principles of good governance, anti-corruption and accountability, and internationally accepted standards governing non-governmental organizations, humanitarian organizations and development partners.

ILA shall conduct its operations in compliance with all applicable legal, regulatory and contractual obligations relating to fraud prevention, corruption, financial accountability, procurement, employment, information management and organizational governance.

Without limiting the general application of this Policy, ILA shall implement this Policy consistently with applicable laws governing:

a) anti-corruption and economic crimes;

b) financial management and accountability;

c) non-governmental organizations and charitable institutions;

d) employment and labour relations;

e) procurement and contract management;

f) taxation and financial reporting;

g) information management and data protection;

h) criminal offences relating to fraud, theft, forgery, bribery, embezzlement and abuse of office;

i) anti-money laundering and countering the financing of terrorism, where applicable;

j) any other legal or regulatory requirements applicable to the operations of ILA.

Where legislative requirements are amended, repealed or replaced, this Policy shall be interpreted and implemented in accordance with the prevailing legal framework.

Where a provision of this Policy conflicts with mandatory legal requirements, the applicable law shall prevail to the extent of the inconsistency, while the remaining provisions of this Policy shall continue to apply.

ILA shall cooperate fully with competent government institutions, oversight bodies and law enforcement agencies in accordance with applicable laws whenever criminal conduct or regulatory breaches are identified.

1.9 International Standards

ILA recognizes that many of its programmes are implemented with financial and technical support from national and international development partners. Accordingly, this Policy is informed by internationally recognized principles and standards relating to integrity, accountability, anti-corruption and organizational governance.

In implementing this Policy, ILA shall, where applicable, be guided by:

a) the **United Nations Convention against Corruption (UNCAC)**;

b) the **United Nations Convention against Transnational Organized Crime**, where relevant;

c) the **United Nations Sustainable Development Goals (SDGs)**, particularly Goal 16 on Peace, Justice and Strong Institutions;

d) internationally recognized principles of transparency, accountability and good governance applicable to civil society organizations;

e) international anti-bribery and anti-corruption standards, including the principles reflected in **ISO 37001 Anti-Bribery Management Systems**, where appropriate;

f) internationally accepted internal control and enterprise risk management principles, including the **COSO Internal Control Framework** and related guidance;

g) donor compliance requirements applicable to ILA-funded programmes, including financial management, procurement, safeguarding, audit, reporting and fraud notification obligations;

h) ethical standards applicable to legal aid providers, human rights organizations and humanitarian actors;

i) internationally recognized principles relating to whistleblower protection, accountability and organizational transparency.

Where donor agreements prescribe higher standards than those contained in this Policy, ILA shall comply with the higher standard to the extent that it is lawful and operationally feasible.

Nothing in this Policy shall prevent ILA from adopting additional integrity measures that strengthen organizational accountability beyond the minimum legal or donor requirements.

1.10 Relationship with Other ILA Policies

This Policy forms part of ILA's integrated governance, compliance and internal control framework and shall be read together with other organizational policies, procedures and operational manuals.

This Policy complements, and where appropriate shall be implemented alongside, the following documents:

a) Finance and Accounting Policy;

b) Procurement and Asset Management Policy;

c) Human Resource and Administration Policy and Manual;

d) Code of Conduct and Ethics Policy;

e) Risk Management Policy;

f) ICT Policy;

g) Data Protection and Privacy Policy;

h) Prevention of Sexual Exploitation, Abuse and Harassment (PSEAH) Policy;

i) Safeguarding Policy;

j) Monitoring, Evaluation, Accountability and Learning (MEAL) Policy;

k) Partnership Management Policy;

l) Grant Management Policy;

m) Records and Information Management Policy;

n) any other policy approved by the Board of Directors.

Where an incident falls within the scope of more than one policy, the relevant policies shall be applied concurrently to ensure comprehensive and appropriate management of the matter.

For example:

- allegations involving procurement fraud shall be addressed together with the Procurement and Asset Management Policy;

- financial irregularities shall be addressed together with the Finance and Accounting Policy;
- misconduct by employees shall also be managed in accordance with the Human Resource and Administration Policy;
- data-related misconduct shall additionally be addressed under the Data Protection and Privacy Policy and ICT Policy;
- safeguarding-related misconduct shall also be managed under the Safeguarding Policy and PSEAH Policy.

Nothing in this Policy limits the authority of ILA to apply other policies or legal procedures where appropriate.

1.11 Policy Ownership

The Board of Directors is the owner of this Policy and retains ultimate responsibility for ensuring that ILA maintains an effective anti-fraud, anti-corruption and whistleblowing framework.

The Board shall exercise strategic oversight by:

a) approving this Policy and subsequent amendments;

b) ensuring that adequate governance arrangements exist to prevent fraud and corruption;

c) promoting a culture of integrity throughout the organization;

d) overseeing significant fraud and corruption risks;

e) reviewing reports relating to serious fraud incidents;

f) ensuring management implements effective corrective actions;

g) holding executive management accountable for implementation of this Policy.

The Executive Director shall be the Policy Custodian and shall be responsible for the day-to-day implementation, administration and enforcement of this Policy throughout the organization.

Departmental managers shall be responsible for implementing this Policy within their respective areas of responsibility and ensuring that appropriate controls are established and maintained.

Every person associated with ILA shares responsibility for safeguarding organizational resources and complying with this Policy.

1.12 Policy Administration

The Executive Director shall designate an appropriate office, department or responsible officer to coordinate implementation of this Policy.

Policy administration shall include:

a) coordinating fraud prevention initiatives;

b) maintaining fraud and corruption reporting mechanisms;

c) coordinating awareness and training programmes;

d) maintaining registers relating to fraud incidents, whistleblower reports and conflict of interest declarations;

e) supporting investigations and follow-up actions;

f) coordinating institutional risk assessments relating to fraud and corruption;

g) monitoring compliance with this Policy;

h) preparing periodic implementation reports for senior management and the Board of Directors;

i) recommending improvements based on audits, investigations and organizational learning.

All departments shall cooperate in implementing this Policy and shall provide information, documentation and assistance necessary for effective administration.

Where specialized expertise is required, ILA may engage independent investigators, auditors, legal advisers or other qualified professionals to support implementation of this Policy.

1.13 Effective Date

This Policy shall become effective upon its approval by the Board of Directors of the Initiative for Legal Aid (ILA).

Upon approval:

a) this Policy shall supersede any previous internal guidelines relating to anti-fraud, anti-corruption and whistleblowing, to the extent of any inconsistency;

b) all staff members and other persons covered by this Policy shall be informed of its adoption;

c) managers shall ensure that the Policy is incorporated into operational procedures, staff induction programmes and organizational governance systems;

d) relevant contractual documents, partnership agreements and procurement documents shall, where appropriate, be updated to reflect compliance obligations under this Policy.

Implementation of this Policy shall commence immediately unless otherwise determined by the Board of Directors.

1.14 Policy Review

ILA recognizes that fraud risks, legal requirements, donor expectations and organizational operations evolve over time. Accordingly, this Policy shall be subject to regular review to ensure that it remains effective, practical and aligned with best practices.

The Policy shall ordinarily be reviewed every **three (3) years**, or earlier where circumstances require.

An earlier review may be initiated where:

a) significant fraud or corruption incidents occur;

b) major organizational restructuring takes place;

c) new legislation or regulatory requirements are enacted;

d) donor requirements or contractual obligations change;

e) audits or investigations identify significant weaknesses;

f) emerging fraud risks require additional controls;

g) the Board of Directors determines that amendments are necessary.

The review process shall include, where appropriate:

- consultation with management and relevant departments;
- consideration of audit findings and investigation reports;
- analysis of fraud trends and organizational risk assessments;
- lessons learned from implementation;
- stakeholder feedback;
- benchmarking against recognized national and international good practices.

Any proposed amendment shall be submitted to the Board of Directors for approval in accordance with ILA's governance procedures.

Until formally amended or replaced, this Policy shall remain in full force and effect.

CHAPTER TWO

PURPOSE, OBJECTIVES AND SCOPE OF THE POLICY

2.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that fraud, corruption, bribery and other forms of unethical conduct pose significant risks to organizational integrity, financial sustainability, programme effectiveness and public confidence. These risks may result in financial losses, damage to institutional reputation, reduced donor confidence, legal liability and diminished trust among beneficiaries and stakeholders.

This Chapter establishes the purpose, objectives, scope and institutional application of this Policy. It clarifies the persons, activities and resources covered by the Policy and outlines the fundamental responsibilities of all individuals associated with ILA in preventing, detecting and responding to fraud and corruption.

This Chapter shall be read together with the remaining provisions of this Policy and other related organizational policies, procedures and applicable laws.

2.2 Purpose of the Policy

The primary purpose of this Policy is to establish a comprehensive framework for preventing, detecting, reporting, investigating and responding to fraud, corruption, bribery and related misconduct within Initiative for Legal Aid (ILA).

The Policy seeks to:

a) safeguard the financial, physical, technological and intellectual resources of ILA;

b) promote integrity, honesty and accountability throughout the organization;

c) strengthen internal control systems that minimize opportunities for fraud and corruption;

d) provide safe, confidential and accessible mechanisms for reporting suspected misconduct;

e) protect whistleblowers and other persons who report concerns in good faith;

f) establish fair and transparent procedures for investigating allegations;

g) ensure appropriate disciplinary, administrative and legal action where misconduct is established; and

h) promote public confidence in the governance and operations of ILA.

2.3 Policy Objectives

The objectives of this Policy are to:

a) establish clear standards of ethical conduct applicable to all persons associated with ILA;

b) prevent fraud, corruption and abuse of organizational resources;

c) strengthen systems of internal accountability and financial integrity;

d) ensure compliance with applicable laws, donor requirements and organizational policies;

e) promote transparency in organizational decision-making;

f) encourage early identification and reporting of misconduct;

g) protect organizational assets and donor resources;

h) foster a culture of openness, responsibility and ethical leadership;

i) ensure allegations of misconduct are addressed promptly, fairly and objectively; and

j) support continuous institutional improvement through lessons learned and risk management.

2.4 Scope of the Policy

This Policy applies to all activities undertaken by or on behalf of Initiative for Legal Aid, irrespective of the funding source, geographical location or mode of implementation.

The Policy governs conduct relating to:

a) governance activities;

b) programme implementation;

c) legal aid service delivery;

d) financial management;

e) procurement and contract management;

f) recruitment and human resource management;

g) partnership and grant management;

h) project implementation;

i) monitoring, evaluation and reporting;

j) management of information and technology systems; and

k) any other activity undertaken in the name of ILA.

2.5 Persons Covered by the Policy

This Policy applies to every individual acting for or on behalf of ILA, including but not limited to:

a) members of the Board of Directors;

b) the Executive Director;

c) senior management;

d) employees, whether permanent, temporary or casual;

e) interns and volunteers;

f) consultants;

g) contractors;

h) suppliers and vendors;

i) implementing partners and sub-grantees;

j) community-based workers;

k) experts and advisers;

l) agency personnel engaged by ILA; and

m) any other individual representing or acting on behalf of the organization.

Compliance with this Policy shall form part of the contractual and ethical obligations of all covered persons.

2.6 Organizational Resources Covered

For purposes of this Policy, organizational resources include, but are not limited to:

a) financial resources;

b) donor funds;

c) grants and project resources;

d) vehicles;

e) office equipment;

f) computers and ICT systems;

g) furniture and office facilities;

h) confidential information;

i) electronic data;

j) organizational records;

k) intellectual property;

l) legal documents;

m) organizational identity, logo and reputation; and

n) any other tangible or intangible asset owned, controlled or managed by ILA.

2.7 Institutional Commitment

ILA is committed to maintaining an organizational environment founded upon integrity, accountability, professionalism and transparency.

The organization shall:

a) maintain effective governance systems;

b) establish strong internal controls;

c) promote ethical leadership;

d) encourage responsible stewardship of resources;

e) support whistleblowing and accountability mechanisms;

f) investigate allegations fairly and independently; and

g) continuously improve fraud prevention systems.

2.8 Zero-Tolerance Commitment

ILA adopts a strict zero-tolerance approach towards:

a) fraud;

b) corruption;

c) bribery;

d) theft;

e) embezzlement;

f) abuse of authority;

g) financial misconduct;

h) procurement fraud;

i) conflict of interest violations;

j) retaliation against whistleblowers; and

k) any other conduct that undermines the integrity of the organization.

No person shall be exempt from accountability because of position, seniority or influence.

2.9 Duty to Prevent Fraud and Corruption

Every person covered by this Policy has an individual responsibility to prevent fraud and corruption.

This duty includes:

a) complying with organizational policies;

b) exercising due care in performing assigned duties;

c) protecting organizational resources;

d) reporting suspected misconduct;

e) avoiding conflicts of interest;

f) cooperating with audits and investigations; and

g) promoting ethical conduct within the workplace.

2.10 Relationship with Other Organizational Policies

This Policy shall be implemented together with other organizational policies, including:

a) Finance and Accounting Policy;

b) Procurement and Asset Management Policy;

c) Human Resource and Administration Manual;

d) Code of Conduct and Ethics Policy;

e) Risk Management Policy;

f) ICT Policy;

g) Data Protection and Privacy Policy;

h) PSEAH Policy;

i) MEAL Policy; and

j) Safeguarding Policy.

Where another organizational policy provides more specific procedures relating to a particular matter, both policies shall be read together to ensure comprehensive compliance.

2.11 Compliance with Laws and Donor Requirements

ILA shall implement this Policy in accordance with:

a) the Constitution and laws of the Republic of South Sudan;

b) applicable labour, criminal, procurement and financial legislation;

c) donor contractual obligations;

d) international anti-corruption principles;

e) good governance standards; and

f) recognized NGO accountability frameworks.

Where donor requirements establish higher standards than this Policy, the higher standard shall apply to the extent permitted by law.

2.12 Individual Accountability

Every person covered by this Policy shall be personally accountable for complying with its provisions.

Ignorance of this Policy shall not excuse misconduct.

Individuals shall remain responsible for:

a) understanding their obligations;

b) complying with approved procedures;

c) seeking guidance where uncertainty exists;

d) acting honestly in all organizational dealings; and

e) reporting suspected violations without unreasonable delay.

2.13 Consequences of Non-Compliance

Failure to comply with this Policy may result in one or more of the following actions, depending on the nature and seriousness of the violation:

a) counselling or corrective guidance;

b) written warning;

c) disciplinary proceedings;

d) suspension;

e) termination of employment or contract;

f) recovery of financial losses;

g) removal from organizational responsibilities;

h) debarment from future engagement with ILA;

i) referral to law enforcement authorities; and

j) civil or criminal proceedings where applicable.

2.14 Policy Interpretation

Questions concerning the interpretation or application of this Policy shall be referred to the Executive Director or such other officer designated by the Board of Directors.

Where ambiguity exists, the interpretation that best promotes integrity, accountability, transparency and protection of organizational resources shall prevail.

Nothing in this Policy limits the authority of the Board of Directors to issue additional guidance, directives or implementation procedures consistent with the objectives of this Policy.

2.15 Review of Chapter Implementation

ILA shall periodically assess the effectiveness of the principles contained in this Chapter as part of its broader organizational governance and risk management framework.

The review shall consider:

a) changes in organizational operations;

b) emerging fraud and corruption risks;

c) lessons arising from investigations and audits;

d) recommendations from donors and oversight bodies;

e) amendments to applicable laws and regulations; and

f) best practices in anti-fraud, anti-corruption and whistleblowing governance.

Findings from such reviews shall inform amendments to this Policy, strengthen institutional controls and promote continuous improvement in organizational integrity and accountability.

CHAPTER THREE

DEFINITIONS, INTERPRETATION AND KEY CONCEPTS

3.1 Definitions

For the purposes of this Anti-Fraud, Corruption and Whistleblowing Policy, the following words and expressions shall have the meanings assigned to them in this Chapter unless the context otherwise requires. These definitions are intended to promote a common understanding of key concepts, ensure consistent interpretation and facilitate the effective implementation of this Policy.

Where a term is not specifically defined in this Policy, it shall be interpreted in accordance with the applicable laws of the Republic of South Sudan, relevant donor requirements, internationally recognized anti-corruption standards and other applicable ILA policies.

The definitions contained in this Chapter shall apply throughout this Policy and to all persons covered under it.

3.2 Fraud

Fraud means any intentional act, omission, deception, concealment, misrepresentation or abuse of trust designed to obtain an unlawful, unauthorized or unfair financial, material, personal or organizational benefit, or to cause loss to another person or entity.

Fraud may be committed by employees, Board members, volunteers, consultants, contractors, suppliers, implementing partners, beneficiaries or any person acting on behalf of ILA.

Fraud includes, but is not limited to:

a) falsification of financial records;

b) submission of false invoices, receipts or payment vouchers;

c) alteration or destruction of official records;

d) false claims for reimbursement;

e) manipulation of payroll records;

f) creation of fictitious suppliers or beneficiaries;

g) concealment of material information;

h) forgery of signatures or official documents;

i) unauthorized diversion of organizational resources; and

j) any other dishonest act intended to obtain improper benefit.

3.3 Corruption

Corruption means the abuse of entrusted power, authority or position for private gain, personal benefit or the benefit of another person or organization.

Corruption may occur in financial management, procurement, recruitment, programme implementation, partnership management or any organizational activity.

Examples include:

a) accepting or offering bribes;

b) misuse of official authority;

c) favoritism in decision-making;

d) abuse of procurement processes;

e) unlawful influence over recruitment or promotions;

f) diversion of donor resources;

g) manipulation of programme activities for personal benefit; and

h) concealment of corrupt practices.

ILA maintains a zero-tolerance approach to corruption in all its forms.

3.4 Bribery

Bribery means the offering, promising, giving, requesting, receiving or accepting of money, gifts, services, favours or any other thing of value with the intention of improperly influencing an official decision, action or business transaction.

Bribery may occur before, during or after a decision has been made.

Examples include:

a) offering money to obtain a contract;

b) accepting gifts in exchange for procurement decisions;

c) paying an official to overlook non-compliance;

d) providing personal benefits to influence recruitment outcomes; or

e) requesting unofficial payments for services that should be provided without charge.

Both giving and receiving bribes are prohibited under this Policy.

3.5 Theft

Theft means the unlawful taking, removal, appropriation or possession of money, property, equipment, information or other assets belonging to ILA, its partners, donors, beneficiaries or any other stakeholder without authorization.

Theft includes:

a) stealing cash;

b) unauthorized removal of office equipment;

c) theft of laptops, mobile phones or vehicles;

d) unauthorized copying or removal of confidential information;

e) taking supplies intended for programme activities; and

f) unlawful use of organizational assets for private purposes.

3.6 Embezzlement

Embezzlement means the fraudulent appropriation, conversion or misuse of money, assets or property entrusted to an individual by virtue of their employment, appointment or contractual relationship with ILA.

Examples include:

a) diverting donor funds;

b) unauthorized transfers from organizational accounts;

c) misuse of project advances;

d) retaining programme funds for personal use;

e) unauthorized sale of organizational property; and

f) concealment of financial shortages.

3.7 Money Laundering

Money laundering refers to any act intended to conceal, disguise, transfer or legitimize the origin of funds or assets obtained through criminal or unlawful activities.

ILA shall not knowingly receive, process, transfer or use funds derived from illegal activities.

Where suspicious financial transactions are identified, appropriate reporting and legal procedures shall be followed in accordance with applicable laws and donor requirements.

3.8 Facilitation Payments

Facilitation payments are unofficial or unauthorized payments, gifts or benefits made to public officials or other persons to expedite or secure routine administrative actions.

ILA prohibits facilitation payments except where:

a) payment is expressly required by law;

b) official government receipts are issued;

c) the payment has been properly authorized under organizational procedures.

Any request for an improper facilitation payment shall be reported immediately.

3.9 Conflict of Interest

A conflict of interest exists where an individual's personal, financial, family, political, business or other private interests interfere, or appear to interfere, with their ability to act objectively and in the best interests of ILA.

Conflicts of interest may be:

a) actual;

b) potential; or

c) perceived.

All conflicts shall be declared promptly and managed in accordance with this Policy.

3.10 Abuse of Authority

Abuse of authority means the improper use of official position, influence or organizational power for personal benefit or to improperly influence decisions affecting others.

Examples include:

a) intimidating staff;

b) interfering with investigations;

c) bypassing established procedures;

d) coercing subordinates to violate policies;

e) using organizational authority for private advantage; and

f) shielding individuals from accountability.

3.11 Nepotism

Nepotism refers to granting employment, contracts, promotions, benefits or other organizational opportunities to relatives or family members without following fair, transparent and competitive procedures.

Nepotism undermines merit-based decision-making and increases organizational risk.

ILA prohibits nepotism in all organizational processes.

3.12 Favoritism

Favoritism means providing unfair preference or advantage to individuals based on friendship, personal relationships, political affiliation, ethnicity, social connections or other non-merit considerations.

Organizational decisions shall always be based upon competence, fairness, transparency and organizational interests.

3.13 Extortion

Extortion means obtaining money, property, services, favours or other benefits through threats, coercion, intimidation, abuse of authority or unlawful pressure.

Examples include:

a) demanding payment before providing services;

b) threatening disciplinary action unless benefits are received;

c) forcing suppliers to provide unofficial payments;

d) coercing beneficiaries into providing money or gifts.

Extortion constitutes serious misconduct and may amount to a criminal offence.

3.14 Collusion

Collusion refers to secret or improper cooperation between two or more persons intended to manipulate organizational processes or obtain an unfair advantage.

Collusion may occur between:

a) employees;

b) suppliers;

c) contractors;

d) consultants;

e) procurement committee members; or

f) external partners.

Examples include bid-rigging, price fixing and coordinated submission of fraudulent quotations.

3.15 Kickbacks

Kickbacks are secret commissions, payments, gifts or other benefits given or received in exchange for awarding contracts, approving payments, influencing procurement decisions or facilitating improper business advantages.

Kickbacks are strictly prohibited irrespective of their value.

3.16 Procurement Fraud

Procurement fraud means any dishonest act intended to manipulate procurement processes or obtain improper advantage during acquisition of goods, works or services.

Examples include:

a) false quotations;

b) inflated pricing;

c) supplier collusion;

d) bid manipulation;

e) false delivery certificates;

f) unauthorized contract variations;

g) splitting procurements to avoid approval thresholds; and

h) procurement involving undisclosed conflicts of interest.

3.17 Payroll Fraud

Payroll fraud refers to dishonest manipulation of payroll systems resulting in unauthorized salary payments or benefits.

Examples include:

a) creation of ghost employees;

b) falsified attendance records;

c) unauthorized salary adjustments;

d) duplicate salary payments;

e) manipulation of overtime claims; and

f) payment of fictitious allowances.

3.18 Cyber Fraud

Cyber fraud means fraudulent activities committed through electronic systems, computer networks, digital platforms or information technology resources.

Examples include:

a) unauthorized access to organizational systems;

b) phishing attacks;

c) electronic payment fraud;

d) hacking;

e) identity theft through electronic means;

f) alteration of electronic financial records; and

g) fraudulent use of organizational email accounts.

3.19 Identity Fraud

Identity fraud means the unlawful use, theft, falsification or impersonation of another person's identity or official credentials for fraudulent purposes.

Examples include:

a) impersonating staff members;

b) using forged identification documents;

c) creating false user accounts;

d) unauthorized use of official passwords or digital credentials.

3.20 Whistleblower

A whistleblower is any individual who, in good faith, reports suspected fraud, corruption, misconduct or violations of this Policy.

A whistleblower may include:

a) Board members;

b) employees;

c) volunteers;

d) consultants;

e) contractors;

f) suppliers;

g) beneficiaries;

h) implementing partners; or

i) members of the public.

A whistleblower is not required to prove wrongdoing before making a report but should have reasonable grounds for concern.

3.21 Good Faith

Good faith means an honest belief, based on reasonable grounds, that information provided concerning suspected misconduct is true or likely to be true.

A report made in good faith shall remain protected even where an investigation ultimately concludes that insufficient evidence exists to substantiate the allegation.

Knowingly false or malicious reports are not protected.

3.22 Retaliation

Retaliation means any adverse action taken against a person because they have reported suspected misconduct, cooperated with an investigation or supported accountability processes.

Retaliation includes:

a) dismissal;

b) demotion;

c) harassment;

d) intimidation;

e) discrimination;

f) reduction of benefits;

g) workplace isolation;

h) threats; or

i) any other adverse treatment.

Retaliation is strictly prohibited and constitutes a separate violation of this Policy.

3.23 Investigation

An investigation is a structured, impartial and confidential process undertaken to establish facts concerning allegations of fraud, corruption or other misconduct.

Investigations shall aim to:

a) establish the facts;

b) preserve evidence;

c) determine responsibility;

d) assess losses;

e) recommend corrective measures; and

f) strengthen organizational controls.

Investigations shall be conducted fairly, independently, objectively and in accordance with due process.

3.24 Corrective Action

Corrective action means any administrative, operational, disciplinary or procedural measure implemented to address identified misconduct, remedy weaknesses and prevent recurrence.

Corrective actions may include:

a) policy revisions;

b) staff training;

c) strengthening internal controls;

d) disciplinary measures;

e) recovery of losses;

f) contract termination;

g) enhanced supervision; and

h) referral to competent authorities.

3.25 Recovery

Recovery means the process of reclaiming, reimbursing or restoring financial resources, assets, property or other losses arising from fraud, corruption or misconduct.

Recovery measures may include:

a) restitution by the responsible individual;

b) recovery of misappropriated assets;

c) deductions permitted by law or contract;

d) civil recovery proceedings;

e) insurance claims where applicable;

f) recovery through contractual remedies; and

g) any other lawful mechanism available to restore organizational losses.

ILA shall take all reasonable and lawful steps to recover funds and assets lost through fraud, corruption or related misconduct, while ensuring that recovery efforts are proportionate, properly documented and consistent with applicable laws and contractual obligations.

CHAPTER FOUR

FRAUD RISK MANAGEMENT FRAMEWORK

4.1 Fraud Risk Philosophy

Initiative for Legal Aid (ILA) recognizes that fraud risks exist in every organization regardless of its size, structure or operational environment. As a legal aid and human rights organization entrusted with donor funds, public confidence and community trust, ILA is committed to proactively identifying, assessing and managing fraud risks before they result in financial loss, operational disruption or reputational damage.

ILA adopts a **risk-based approach** to fraud prevention that emphasizes prevention over reaction. Rather than responding only after fraud has occurred, the organization shall continuously identify vulnerabilities, strengthen internal controls and promote an ethical culture that discourages fraudulent and corrupt conduct.

The organization's fraud risk philosophy is guided by the following principles:

a) fraud prevention is more effective and economical than fraud detection after losses have occurred;

b) fraud risk management is a shared organizational responsibility;

c) fraud risks shall be integrated into the organization's overall Risk Management Framework;

d) internal controls shall be proportionate to the level of identified risk;

e) transparency, accountability and ethical leadership are essential components of fraud prevention;

f) fraud risks shall be reviewed continuously as organizational activities evolve; and

g) management decisions shall be informed by evidence-based fraud risk assessments.

ILA shall cultivate an organizational culture in which fraud risks are openly discussed, promptly reported and effectively managed without fear or favour.

4.2 Fraud Risk Identification

ILA shall establish systematic processes for identifying actual, potential and emerging fraud risks across all organizational operations, programmes and support functions.

Fraud risk identification shall be undertaken:

a) during strategic planning;

b) before commencement of new projects;

c) during programme implementation;

d) before entering partnership agreements;

e) during procurement planning;

f) when introducing new financial systems;

g) during restructuring or organizational change; and

h) following incidents of fraud or significant control failures.

Fraud risks may arise from, among others:

- weak internal controls;
- inadequate segregation of duties;
- poor supervision;
- ineffective procurement practices;
- cash handling processes;
- payroll administration;
- grant management;
- procurement and logistics;
- asset management;
- information technology systems;
- recruitment processes;
- partnership management;
- beneficiary registration;
- donor reporting;
- banking and payment systems;
- cyber security threats.

Methods for identifying fraud risks may include:

a) fraud risk workshops;

b) staff consultations;

c) internal audit findings;

d) external audit recommendations;

e) management reviews;

f) donor assessments;

g) complaints and whistleblower reports;

h) monitoring and evaluation findings;

i) lessons learned from previous fraud cases; and

j) environmental scanning for emerging fraud trends.

All departments shall participate actively in fraud risk identification within their respective areas of responsibility.

4.3 Fraud Risk Assessment

Following identification, fraud risks shall be assessed to determine their likelihood of occurrence and the potential impact on the organization.

The purpose of fraud risk assessment is to enable ILA to allocate resources efficiently and implement controls proportionate to the level of risk.

Each identified fraud risk shall be evaluated based on factors including:

a) likelihood of occurrence;

b) potential financial loss;

c) operational disruption;

d) legal consequences;

e) donor compliance implications;

f) reputational damage;

g) impact on beneficiaries;

h) effect on programme delivery; and

i) existing control effectiveness.

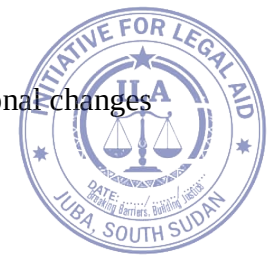
Risk assessments shall consider both:

- inherent risk (before controls); and
- residual risk (after existing controls are considered).

ILA may classify fraud risks using categories such as:

- Very High Risk;
- High Risk;
- Moderate Risk;
- Low Risk; and
- Minimal Risk.

Risk assessments shall be documented and reviewed whenever significant operational changes occur.



4.4 Fraud Risk Register

ILA shall establish and maintain a comprehensive Fraud Risk Register as part of its organizational risk management system.

The Fraud Risk Register shall serve as the official record of identified fraud risks and corresponding management actions.

The Register shall, where appropriate, include:

a) reference number;

b) description of the fraud risk;

c) affected department or programme;

d) source of the risk;

e) existing controls;

f) likelihood rating;

g) impact rating;

h) overall risk rating;

i) additional mitigation measures required;

j) responsible officer;

k) implementation timeline;

l) review date; and

m) status of mitigation actions.

The Fraud Risk Register shall be:

- reviewed regularly;
- updated whenever new risks emerge;
- available to authorized management personnel;
- integrated with ILA's organizational Risk Register where appropriate.

Confidentiality shall be maintained where disclosure of risk information may compromise investigations or organizational security.

4.5 Risk Prioritization

ILA recognizes that not all fraud risks require the same level of response. Identified risks shall therefore be prioritized according to their significance and potential impact on the organization.

Priority shall be determined by considering:

a) severity of potential consequences;

b) likelihood of occurrence;

c) vulnerability of existing controls;

d) financial exposure;

e) donor sensitivity;

f) programme importance;

g) legal obligations; and

h) urgency of corrective action.

Fraud risks classified as High or Very High shall receive immediate management attention.

Risk prioritization shall assist management in:

- allocating resources efficiently;
- strengthening high-risk controls;
- scheduling audits;
- planning monitoring activities;
- determining investigation priorities; and
- improving oversight.

Risk prioritization shall remain dynamic and be reviewed whenever circumstances change.

4.6 Risk Mitigation

ILA shall implement appropriate preventive, detective and corrective measures to reduce identified fraud risks to acceptable levels.

Risk mitigation measures may include:

a) strengthening internal controls;

b) segregation of duties;

c) approval hierarchies;

d) financial reconciliations;

e) procurement oversight;

f) conflict of interest declarations;

g) staff rotation where appropriate;

h) mandatory leave for key finance personnel where feasible;

i) improved supervision;

j) access controls for ICT systems;

k) enhanced documentation requirements;

l) supplier due diligence;

m) beneficiary verification;

n) independent audits;

o) whistleblowing mechanisms;

p) fraud awareness training;

q) data analytics and transaction monitoring; and

r) continuous policy review.

Management shall ensure that mitigation measures are practical, proportionate, cost-effective and regularly evaluated for effectiveness.

4.7 Risk Monitoring

Fraud risk management is a continuous process requiring ongoing monitoring of identified risks, implemented controls and emerging threats.

ILA shall monitor fraud risks through:

a) internal audits;

b) management reviews;

c) financial monitoring;

d) procurement reviews;

e) programme monitoring visits;

f) donor compliance reviews;

g) spot checks;

h) asset verification exercises;

i) ICT security monitoring;

j) whistleblower reports;

k) investigation findings; and

l) periodic fraud risk reassessments.

Monitoring activities shall evaluate whether:

- identified risks remain relevant;
- controls are functioning effectively;
- additional controls are required;
- new fraud risks have emerged; and
- corrective actions have been implemented.

Departments shall promptly report significant changes affecting fraud risks.

4.8 Risk Reporting

Effective fraud risk management requires timely, accurate and transparent reporting to facilitate informed decision-making.

Management shall establish reporting mechanisms that ensure fraud risks are communicated to the appropriate governance levels.

Fraud risk reports may include:

a) newly identified risks;

b) changes in risk ratings;

c) implementation status of mitigation measures;

d) significant control weaknesses;

e) fraud incidents and trends;

f) investigation outcomes;

g) audit recommendations;

h) emerging threats; and

i) management responses.

Depending on the nature of the risk, reports may be submitted to:

- the Executive Director;
- Senior Management Team;
- the Audit or Risk Committee (where established);
- the Board of Directors; and
- donors or regulatory authorities where required by contractual obligations or law.

Fraud risk reporting shall respect confidentiality and the rights of individuals while ensuring organizational accountability.

4.9 Continuous Improvement

ILA recognizes that fraud risks evolve continuously due to changes in technology, operational environments, funding arrangements and external threats.

Accordingly, the organization shall continuously strengthen its fraud risk management framework through regular learning, evaluation and improvement.

Continuous improvement shall include:

a) reviewing fraud risk assessments periodically;

b) updating the Fraud Risk Register;

c) implementing recommendations arising from investigations;

d) incorporating audit findings into internal controls;

e) monitoring emerging fraud trends;

f) strengthening organizational policies;

g) improving staff capacity through regular training;

h) enhancing information technology security;

i) benchmarking against recognized good practices; and

j) incorporating lessons learned from partners, donors and peer organizations.

The Executive Director shall ensure that fraud risk management remains an integral part of organizational governance, strategic planning and operational decision-making.

Through continuous improvement, ILA shall maintain a resilient fraud prevention framework that protects organizational resources, strengthens donor confidence, safeguards beneficiaries and promotes a culture of integrity, transparency and accountability.

CHAPTER FIVE

FRAUD PREVENTION STRATEGY

5.1 Prevention Framework

The Initiative for Legal Aid (ILA) recognizes that preventing fraud is significantly more effective and less costly than detecting and correcting fraud after it has occurred. Fraud prevention shall therefore be integrated into every aspect of organizational governance, management, operations, financial administration, procurement, human resource management, project implementation, and partnership management.

ILA shall maintain a proactive fraud prevention framework based on internationally recognized principles of good governance, accountability, transparency, internal control, ethical leadership, and risk management.

The fraud prevention framework shall be guided by the following principles:

a. prevention is the responsibility of every employee and representative of ILA;

b. strong internal controls reduce opportunities for fraud;

c. ethical leadership sets the tone for organizational integrity;

d. fraud risks shall be identified before they materialize;

e. prevention measures shall be continuously reviewed and strengthened;

f. donor requirements and legal obligations shall be fully integrated into fraud prevention mechanisms;

g. fraud prevention shall be embedded within planning, budgeting, procurement, finance, human resources, logistics, ICT, legal services, and programme implementation.

The Executive Director shall ensure adequate resources are allocated to fraud prevention activities, including staff awareness, internal controls, audits, monitoring systems, and technological safeguards.

5.2 Ethical Culture

ILA recognizes that organizational culture is the strongest defence against fraud. An ethical culture discourages misconduct by promoting honesty, fairness, accountability, professionalism, and respect for the law.

ILA shall cultivate an ethical culture by:

a. demonstrating integrity through leadership;

b. promoting transparency in decision-making;

c. encouraging staff to report suspected misconduct;

d. rewarding ethical behaviour;

e. maintaining zero tolerance for fraud and corruption;

f. ensuring consistency in disciplinary action;

g. providing ethics and integrity training;

h. integrating ethical values into performance management;

i. communicating organizational values regularly;

j. encouraging open discussion of ethical dilemmas.

Managers shall lead by example and shall not tolerate unethical behaviour regardless of the position of the offender.

Every employee shall sign the Code of Conduct and Ethics Policy upon recruitment and reaffirm compliance whenever required.

5.3 Preventive Controls

ILA shall establish preventive controls designed to reduce opportunities for fraud before losses occur.

Preventive controls shall include, but shall not be limited to:

a. documented policies and procedures;

b. segregation of duties;

c. delegated authority limits;

d. approval hierarchies;

e. procurement controls;

f. payroll verification;

g. inventory controls;

h. bank reconciliations;

i. access controls over information systems;

j. staff vetting and recruitment screening;

k. due diligence for vendors and partners;

l. mandatory supporting documentation for all transactions;

m. regular management reviews;

n. budgeting and expenditure controls;

o. conflict of interest declarations.

Preventive controls shall be reviewed periodically to ensure they remain effective against emerging fraud risks.

5.4 Segregation of Duties

ILA shall ensure that no individual has sole control over an entire financial or operational process.

Critical duties shall be divided among different individuals to minimize the risk of fraud, error, abuse, or unauthorized transactions.

Segregation of duties shall apply to:

a. procurement;

b. payment processing;

c. payroll administration;

d. cash management;

e. banking transactions;

f. inventory management;

g. donor reporting;

h. accounting;

i. project implementation;

j. asset disposal.

Where staffing limitations prevent full segregation of duties, compensating controls shall be implemented, including:

a. enhanced supervisory review;

b. independent reconciliations;

c. periodic internal audits;

d. surprise inspections;

e. additional approval requirements.

No staff member shall authorize, process, verify, and record the same financial transaction.

5.5 Authorization Controls

ILA shall establish formal authorization procedures for all operational and financial transactions.

Authority shall only be exercised by designated officials acting within approved delegated limits.

Authorization controls shall include:

a. documented approval matrices;

b. financial delegation schedules;

c. procurement approval thresholds;

d. contract approval procedures;

e. electronic approval systems where applicable;

f. expenditure approval before commitment of funds;

g. verification of budget availability prior to approval;

h. dual authorization for high-value transactions;

i. Board approval where required by policy.

No employee may approve a transaction in which they have a personal interest.

Unauthorized commitments made on behalf of ILA may result in disciplinary action and personal liability where permitted by law.

5.6 Financial Controls

ILA shall maintain strong financial controls to safeguard organizational resources and donor funds.

Financial controls shall include:

a. annual budgeting;

b. approved chart of accounts;

c. bank reconciliations;

d. monthly financial reporting;

e. periodic management review;

f. expenditure verification;

g. supporting documentation for all payments;

h. restricted access to accounting systems;

i. secure custody of cash and financial records;

j. periodic cash counts;

k. donor fund tracking;

l. asset verification;

m. financial audits;

n. expenditure monitoring against approved budgets;

o. compliance with donor financial regulations.

Payments shall only be made after confirming:

- availability of budget;
- legitimacy of expenditure;
- receipt of goods or services;
- proper authorization;
- supporting documentation.

Cash transactions shall be minimized wherever practicable.

Electronic payments shall be preferred to improve accountability and audit trails.

5.7 Procurement Controls

Procurement activities present a significant fraud risk and shall therefore be governed by robust preventive controls in accordance with ILA's Procurement and Asset Management Policy.

ILA shall ensure that procurement processes are fair, transparent, competitive, and accountable.

Procurement controls shall include:

a. procurement planning;

b. approved procurement methods;

c. competitive bidding;

d. independent bid evaluation committees;

e. supplier due diligence;

f. declaration of conflicts of interest;

g. procurement approval thresholds;

h. contract management procedures;

i. verification of goods and services received;

j. segregation of procurement responsibilities;

k. maintenance of complete procurement records;

l. monitoring supplier performance;

m. prohibition of unauthorized sole-source procurement except where justified and approved;

n. regular procurement audits.

Employees shall not:

a. solicit gifts from suppliers;

b. accept kickbacks;

c. manipulate tender specifications;

d. disclose confidential bid information;

e. split procurements to avoid approval thresholds;

f. collude with suppliers;

g. approve payments for goods not received;

h. create fictitious suppliers.

Any procurement irregularity shall be reported immediately for investigation in accordance with this Policy.

5.8 Human Resource (HR) Controls

ILA recognizes that effective human resource management is a critical component of fraud prevention. Robust HR controls reduce the risk of employing unsuitable individuals, minimize opportunities for misconduct, and promote a culture of integrity and accountability throughout the organization.

The Human Resources Unit shall establish and maintain systems that promote ethical recruitment, transparent employment practices, and continuous monitoring of staff conduct.

HR controls shall include, but not be limited to:

a. merit-based and transparent recruitment processes;

b. verification of academic qualifications, professional credentials, and employment history;

c. reference and background checks for prospective employees, consultants, interns, and volunteers, where appropriate;

d. verification of identity documents before appointment;

e. clear employment contracts outlining duties, ethical obligations, and disciplinary consequences;

f. mandatory signing of the Code of Conduct and Ethics Policy, Conflict of Interest Declaration, and other compliance documents upon engagement;

g. induction training covering fraud prevention, anti-corruption measures, safeguarding, and organizational policies;

h. periodic performance evaluations that include assessment of ethical conduct and compliance;

i. mandatory annual leave to reduce opportunities for concealed fraudulent activities;

j. job rotation for positions identified as high-risk where operationally feasible;

k. timely updating of personnel records;

l. immediate withdrawal of organizational access, assets, and privileges upon termination or separation.

The Human Resources Unit shall work closely with the Finance, Procurement, ICT, and Internal Audit functions to ensure that staffing processes support fraud prevention and organizational accountability.

5.9 Information and Communication Technology (ICT) Controls

ILA shall establish appropriate ICT controls to safeguard electronic information, financial systems, digital assets, and communication platforms from fraud, cybercrime, unauthorized access, and data manipulation.

ICT controls shall include:

a. secure authentication mechanisms, including strong password requirements and multi-factor authentication where appropriate;

b. user access controls based on job responsibilities and the principle of least privilege;

c. segregation of system administration responsibilities;

d. periodic review of user access rights;

e. immediate deactivation of user accounts upon staff separation or role changes;

f. encryption of sensitive organizational information during storage and transmission, where applicable;

g. regular system backups and disaster recovery arrangements;

h. installation and maintenance of antivirus software, firewalls, and other cybersecurity protections;

i. monitoring of system logs to identify unusual or unauthorized activities;

j. timely application of software security updates and patches;

k. secure management of electronic financial transactions and digital approvals;

l. restrictions on the use of unauthorized software, devices, and external storage media;

m. protection against phishing, malware, ransomware, and other cyber threats;

n. secure retention of electronic records in accordance with ILA's Data Protection and ICT Policies.

All users of ILA information systems shall use ICT resources responsibly and shall immediately report suspected cybersecurity incidents or unauthorized access.

Any deliberate manipulation, destruction, or unauthorized disclosure of electronic information shall constitute serious misconduct and may result in disciplinary, civil, or criminal proceedings.

5.10 Physical Security

ILA shall maintain appropriate physical security measures to protect personnel, facilities, equipment, cash, confidential information, and other organizational assets from theft, damage, misuse, or unauthorized access.

Physical security measures shall include:

a. controlled access to offices and restricted areas;

b. visitor registration and identification procedures;

c. secure storage of cash, cheque books, financial records, contracts, and confidential documents;

d. lockable cabinets and secure filing systems;

e. inventory management and asset tagging;

f. physical verification of assets at regular intervals;

g. secure custody of organizational seals, stamps, and official documents;

h. protection of computer equipment, servers, and communication devices;

i. key management and access control procedures;

j. emergency procedures for loss, theft, fire, or security incidents.

Departments responsible for assets shall maintain accurate asset registers and promptly report any loss, theft, or damage.

Employees shall exercise due care when handling organizational property and shall not remove assets from ILA premises without proper authorization.

5.11 Third-Party Due Diligence

ILA recognizes that fraud risks may arise through relationships with suppliers, contractors, consultants, implementing partners, sub-grantees, service providers, donors, and other third parties.

Before entering into any contractual or financial relationship, ILA shall undertake appropriate due diligence proportionate to the level of risk.

Due diligence procedures may include:

a. verification of legal registration and licensing;

b. confirmation of beneficial ownership where appropriate;

c. assessment of financial capacity and operational capability;

d. review of reputation and integrity records;

e. verification against applicable sanctions or debarment lists, where required by law or donor agreements;

f. assessment of previous performance and references;

g. review of conflict of interest risks;

h. confirmation of tax compliance where applicable;

i. evaluation of anti-fraud, anti-corruption, safeguarding, and compliance practices;

j. execution of written agreements containing fraud prevention and compliance clauses.

Contracts with third parties shall include provisions allowing ILA to:

a. monitor performance;

b. review supporting documentation;

c. conduct audits where contractually permitted;

d. terminate agreements in cases of fraud, corruption, or material misconduct;

e. seek recovery of losses arising from fraudulent conduct.

Third parties engaged by ILA shall be expected to uphold standards of integrity consistent with this Policy and other applicable organizational policies.

5.12 Fraud Awareness

ILA shall promote continuous fraud awareness to strengthen the organization's ability to prevent, detect, and respond to fraud and corruption.

Fraud awareness programmes shall ensure that employees and stakeholders understand:

a. the various forms of fraud and corruption;

b. fraud risk indicators and warning signs;

c. reporting mechanisms available within the organization;

d. whistleblower protections;

e. responsibilities under this Policy;

f. ethical standards expected of all personnel;

g. consequences of engaging in fraudulent conduct;

h. donor compliance requirements relating to fraud prevention;

i. emerging fraud risks, including cyber fraud and digital financial crime.

Fraud awareness activities may include:

a. induction programmes for new personnel;

b. periodic refresher training;

c. workshops and seminars;

d. circulation of fraud prevention guidance and alerts;

e. staff meetings addressing integrity and accountability;

f. awareness campaigns during International Anti-Corruption Day and other relevant events;

g. lessons learned from investigations and audits, while maintaining confidentiality.

Managers shall reinforce fraud awareness through regular supervision and discussions during departmental meetings.

ILA shall periodically evaluate the effectiveness of fraud awareness initiatives and update training materials to address evolving fraud risks and changes in applicable laws, donor requirements, and organizational operations.

CHAPTER SIX

PROHIBITED CONDUCT

6.1 Fraud

ILA maintains a zero-tolerance policy towards fraud in all its forms. Every employee, Board member, volunteer, intern, consultant, contractor, partner, supplier, and any other person acting on behalf of the organization is prohibited from engaging in fraudulent conduct.

Fraud includes any intentional act or omission designed to deceive another person or entity for the purpose of obtaining an unlawful, improper, or unfair financial or non-financial benefit, or causing loss to ILA, donors, beneficiaries, government institutions, or any other stakeholder.

Fraudulent conduct may include, but is not limited to:

a. falsifying documents;

b. submitting false claims;

c. creating fictitious transactions;

d. concealing material facts;

e. forging signatures;

f. intentionally providing misleading information;

g. manipulating financial or programme records;

h. obtaining unauthorized payments or benefits.

Any individual found to have committed fraud shall be subject to disciplinary measures, recovery of losses, termination of engagement, referral to law enforcement authorities where appropriate, and any other legal or contractual remedies available to ILA.

6.2 Corruption

ILA strictly prohibits all forms of corruption, whether direct or indirect.

Corruption includes the abuse of entrusted power, authority, position, or influence for personal gain or the benefit of another person or organization.

Prohibited corrupt practices include:

a. soliciting or accepting improper benefits;

b. offering advantages to influence official decisions;

c. misuse of organizational resources;

d. abuse of decision-making authority;

e. diversion of donor or organizational resources;

f. concealment of corrupt activities;

g. facilitating corrupt practices by others.

Employees shall immediately report suspected corruption through the reporting mechanisms established under this Policy.

6.3 Bribery

No person acting on behalf of ILA shall directly or indirectly:

a. offer;

b. promise;

c. give;

d. request;

e. solicit; or

f. accept

any bribe, kickback, commission, gift, favour, hospitality, or other advantage intended to improperly influence a decision, action, or omission.

This prohibition applies equally to dealings with:

a. government officials;

b. judicial officers;

c. law enforcement personnel;

d. suppliers;

e. contractors;

f. consultants;

g. implementing partners;

h. beneficiaries;

i. donors; and

j. any other stakeholder.

Small unofficial payments commonly referred to as facilitation payments are prohibited unless expressly permitted by applicable law in exceptional emergency circumstances involving health or safety.

6.4 Theft

The theft of organizational assets, funds, equipment, information, intellectual property, or any other resource belonging to or entrusted to ILA is strictly prohibited.

Theft includes:

a. stealing cash;

b. unauthorized removal of organizational property;

c. theft of confidential information;

d. theft of donor-funded resources;

e. unauthorized personal use of organizational assets;

f. diversion of supplies or equipment.

Any theft shall be investigated promptly and may result in criminal prosecution where appropriate.

6.5 Misappropriation

No employee or representative of ILA shall intentionally misuse, divert, convert, or improperly utilize organizational resources for unauthorized purposes.

Misappropriation includes:

a. personal use of donor funds;

b. diversion of programme resources;

c. unauthorized expenditure;

d. misuse of vehicles;

e. misuse of office equipment;

f. unauthorized use of organizational bank accounts;

g. improper use of grants.

All organizational resources shall be used solely for legitimate organizational purposes.

6.6 Procurement Fraud

ILA prohibits all forms of procurement fraud throughout the procurement cycle.

Procurement fraud includes:

a. manipulation of procurement specifications;

b. favoritism towards suppliers;

c. splitting procurements to avoid approval thresholds;

d. creation of fictitious suppliers;

e. false quotations;

f. collusion among bidders;

g. kickback arrangements;

h. inflated invoices;

i. payment for goods or services not received;

j. falsification of procurement records.

All procurement activities shall comply with the Procurement and Asset Management Policy and applicable donor procurement requirements.

6.7 Payroll Fraud

Payroll fraud is strictly prohibited.

Payroll fraud includes:

a. creation of ghost employees;

b. falsification of attendance records;

c. unauthorized salary adjustments;

d. manipulation of overtime records;

e. payment to former employees after separation;

f. false payroll deductions;

g. duplicate salary payments;

h. unauthorized allowances or benefits.

The Human Resources and Finance Units shall implement appropriate payroll verification procedures to prevent such fraud.

6.8 Grant Fraud

ILA shall ensure that all grant funds are managed honestly, transparently, and strictly in accordance with donor agreements.

Grant fraud includes:

a. diversion of grant funds;

b. false expenditure reporting;

c. submission of fictitious supporting documents;

d. double charging to multiple donors;

e. misrepresentation of project results;

f. unauthorized budget reallocations;

g. concealment of ineligible expenditures.

Grant funds shall only be used for approved project purposes and in accordance with donor requirements.

6.9 Asset Theft

Employees and other representatives shall not steal, conceal, damage, sell, transfer, or otherwise unlawfully dispose of organizational assets.

Assets include:

a. vehicles;

b. computers;

c. furniture;

d. office equipment;

e. communication devices;

f. inventory;

g. legal publications;

h. programme materials;

i. cash;

j. intellectual property.

Loss of assets shall immediately be reported and investigated.

6.10 Abuse of Authority

Individuals holding supervisory, managerial, fiduciary, or governance responsibilities shall not misuse their authority for personal benefit or to benefit others improperly.

Abuse of authority includes:

a. coercing subordinates;

b. improper interference in procurement or recruitment;

c. misuse of delegated authority;

d. intimidation;

e. retaliation against whistleblowers;

f. unauthorized approval of expenditures;

g. preferential treatment contrary to policy.

Managers are expected to exercise authority responsibly, fairly, and transparently.

6.11 Manipulation of Records

ILA strictly prohibits the creation, alteration, destruction, concealment, or falsification of organizational records for fraudulent or improper purposes.

This includes:

a. accounting records;

b. payroll records;

c. procurement documents;

d. legal case files;

e. donor reports;

f. monitoring and evaluation records;

g. attendance records;

h. electronic data;

i. contracts;

j. financial statements.

Records shall accurately reflect the true nature of organizational activities.

6.12 Bid Rigging

Any arrangement intended to undermine fair competition during procurement is prohibited.

Bid rigging includes:

a. collusion among bidders;

b. predetermined winning bids;

c. market allocation;

d. price fixing;

e. suppression of competitive bids;

f. sharing confidential procurement information.

Employees involved in procurement shall report any suspected bid-rigging activities immediately.

6.13 False Reporting

No person shall intentionally prepare, submit, approve, or distribute false or misleading reports on behalf of ILA.

False reporting includes:

a. inaccurate financial reports;

b. inflated programme achievements;

c. falsified monitoring data;

d. false attendance records;

e. fabricated beneficiary information;

f. misleading donor reports;

g. inaccurate audit responses;

h. manipulated statistical information.

Accuracy and honesty shall govern all organizational reporting.

6.14 Programme Fraud

Programme fraud includes any dishonest act intended to improperly obtain, divert, or misuse resources allocated for programme implementation.

Examples include:

a. creation of fictitious beneficiaries;

b. manipulation of beneficiary selection;

c. falsification of participant attendance;

d. diversion of programme materials;

e. inflated activity costs;

f. false training reports;

g. duplicate claims;

h. manipulation of monitoring results.

Programme staff shall ensure that all activities are implemented with integrity, transparency, and accountability.

6.15 Cyber Fraud

ILA prohibits any fraudulent conduct involving information technology systems, electronic communications, or digital platforms.

Cyber fraud includes:

a. unauthorized system access;

b. phishing;

c. identity theft;

d. electronic payment fraud;

e. manipulation of electronic financial records;

f. unauthorized alteration of databases;

g. malware deployment;

h. theft of electronic information;

i. unauthorized disclosure of confidential data.

All ICT users shall comply with the organization's ICT and Data Protection policies.

6.16 Obstruction of Investigations

No individual shall obstruct, interfere with, delay, or improperly influence any fraud investigation, audit, inspection, or review.

Obstruction includes:

a. destruction of evidence;

b. intimidation of witnesses;

c. providing false information;

d. concealing relevant records;

e. interfering with investigators;

f. refusing lawful access to records without justification;

g. coaching witnesses to provide false testimony.

Obstruction of investigations shall constitute serious misconduct and may result in disciplinary action independent of the underlying allegation.

6.17 Retaliation

ILA strictly prohibits retaliation against any individual who, in good faith:

a. reports suspected fraud or corruption;

b. participates in an investigation;

c. provides evidence or information;

d. refuses to engage in fraudulent conduct;

e. cooperates with auditors, investigators, or regulatory authorities.

Retaliation includes, but is not limited to:

a. dismissal or unfair termination;

b. demotion;

c. harassment or intimidation;

d. discrimination;

e. threats or victimization;

f. reduction of responsibilities without justification;

g. denial of legitimate employment opportunities;

h. any adverse action intended to punish a person for making or supporting a protected disclosure.

Any person who engages in retaliation shall be subject to disciplinary action, including dismissal, and may be held personally liable in accordance with applicable laws and contractual obligations.

CHAPTER SEVEN

CONFLICT OF INTEREST MANAGEMENT

7.1 Policy Principles

The Initiative for Legal Aid (ILA) recognizes that conflicts of interest can undermine organizational integrity, impartiality, accountability, and public confidence. Effective identification and management of conflicts of interest are essential to preventing fraud, corruption, favoritism, and abuse of authority.

ILA shall ensure that all organizational decisions are made solely in the best interests of the organization, its beneficiaries, donors, and stakeholders, free from improper personal, financial, political, or other external influences.

The management of conflicts of interest shall be guided by the following principles:

a. integrity and honesty in all official duties;

b. transparency in decision-making;

c. accountability for personal and professional conduct;

d. fairness and impartiality;

e. protection of donor resources and organizational assets;

f. timely disclosure of actual, potential, and perceived conflicts of interest;

g. appropriate management of disclosed conflicts;

h. compliance with applicable laws, donor requirements, and organizational policies.

Every person acting on behalf of ILA has a continuing duty to avoid situations that create conflicts of interest and to disclose any conflict immediately upon becoming aware of it.

7.2 Disclosure Requirements

All Board members, employees, volunteers, interns, consultants, contractors, and other representatives of ILA shall disclose any actual, potential, or perceived conflict of interest that could influence, or reasonably appear to influence, the impartial performance of their duties.

Disclosure shall be made:

a. upon appointment or engagement;

b. annually through a formal declaration process;

c. whenever circumstances change;

d. before participating in any decision where a conflict may arise;

e. immediately upon becoming aware of a new conflict.

Disclosure shall include, where applicable:

a. financial interests;

b. ownership of businesses;

c. directorships or trusteeships;

d. close family relationships;

e. employment outside ILA;

f. consultancy arrangements;

g. significant investments;

h. personal relationships affecting official duties;

i. any other interest that could reasonably be perceived to compromise impartiality.

Failure to disclose a conflict of interest may constitute misconduct and may result in disciplinary action.

7.3 Register of Interests

ILA shall maintain a confidential Register of Interests to record all disclosed interests and conflicts of interest.

The Register shall be maintained by the Human Resources Unit or another designated office authorized by the Executive Director.

The Register shall include, where appropriate:

a. name and position of the individual;

b. nature of the declared interest;

c. date of disclosure;

d. assessment of the conflict;

e. management measures implemented;

f. review dates;

g. closure or resolution of the conflict.

Access to the Register shall be restricted to authorized officials with legitimate organizational responsibilities, while respecting applicable privacy and confidentiality requirements.

The Register shall be reviewed periodically to ensure that declared interests remain current and appropriately managed.

7.4 Gifts and Hospitality

ILA prohibits the acceptance, offering, or solicitation of gifts, hospitality, entertainment, favors, or other benefits that could improperly influence, or appear to influence, organizational decisions or create an obligation toward another party.

Personnel shall not:

a. request gifts or personal favors from suppliers, contractors, beneficiaries, or partners;

b. accept cash or cash equivalents under any circumstances;

c. receive excessive or lavish hospitality;

d. accept gifts intended to influence procurement, recruitment, grant management, legal representation, or other official decisions.

Modest gifts or hospitality of nominal value that are consistent with customary courtesy and do not compromise impartiality may be accepted only where permitted by organizational policy and applicable law.

Where a gift cannot reasonably be declined due to cultural or diplomatic considerations, the recipient shall promptly declare it to the Executive Director or designated authority. The organization shall determine whether the gift should be retained by ILA, donated, returned, or otherwise managed appropriately.

A Gifts and Hospitality Register shall be maintained to record all reportable gifts and hospitality.

7.5 Related Party Transactions

ILA shall ensure that all transactions involving related parties are conducted transparently, fairly, and in the best interests of the organization.

Related parties may include:

a. Board members;

b. senior management;

c. employees;

d. close family members of the above;

e. organizations owned, controlled, or significantly influenced by such persons.

Related party transactions shall:

a. be fully disclosed before approval;

b. be independently reviewed;

c. be conducted on fair and reasonable terms;

d. comply with procurement and financial policies;

e. avoid preferential treatment;

f. be properly documented and recorded.

Any individual with a related party interest shall not participate in discussions, recommendations, evaluations, negotiations, approvals, or supervision relating to that transaction.

Failure to disclose a related party relationship may constitute fraud or misconduct.

7.6 Outside Employment

Employees shall devote their official working time and professional efforts to the duties assigned by ILA and shall avoid outside employment or business activities that conflict with their responsibilities to the organization.

Outside employment shall not:

a. interfere with official duties;

b. compete with ILA's interests or activities;

c. involve misuse of organizational resources;

d. create conflicts of interest;

e. compromise confidentiality;

f. adversely affect the reputation of ILA.

Employees intending to undertake outside employment, consultancy, or business activities that may give rise to a conflict shall obtain prior written approval from the Executive Director or other authorized official.

ILA reserves the right to require modification or discontinuation of outside activities that present unacceptable conflicts of interest.

7.7 Political Activities

ILA is committed to maintaining its independence, impartiality, and non-partisan character.

Personnel are entitled to participate in lawful political activities in their personal capacity; however, such activities shall not interfere with official duties or compromise the neutrality of the organization.

No person shall:

a. use ILA resources to support political parties, candidates, or campaigns;

b. represent personal political views as those of ILA;

c. engage in political campaigning during official working hours;

d. use organizational premises, equipment, or funds for political purposes without lawful authorization;

e. discriminate against any individual based on political affiliation.

Personnel occupying positions that require strict neutrality shall exercise additional caution to avoid any appearance of political bias.

7.8 Family Relationships

ILA recognizes that family or close personal relationships may create actual, potential, or perceived conflicts of interest.

Employees and Board members shall disclose family relationships where such relationships could influence organizational decisions.

Family relationships requiring disclosure may include spouses, domestic partners, parents, children, siblings, in-laws, or other close relatives where the relationship is relevant to official responsibilities.

Individuals shall not:

a. directly supervise close family members;

b. participate in recruitment decisions involving family members;

c. approve payments or benefits for close relatives;

d. participate in procurement decisions involving family-owned businesses;

e. influence disciplinary or performance decisions affecting family members.

Appropriate management measures shall be implemented where family relationships cannot reasonably be avoided.

7.9 Procurement Conflicts

All personnel involved in procurement shall perform their duties impartially and shall avoid situations that create actual, potential, or perceived conflicts of interest.

Individuals participating in procurement processes shall:

a. complete conflict of interest declarations before participating in evaluations or award decisions;

b. immediately disclose any relationship with bidders, suppliers, contractors, or consultants;

c. withdraw from procurement processes where conflicts exist;

d. refrain from accessing confidential procurement information where disqualified;

e. avoid any communication with bidders that could compromise fairness or transparency.

Procurement conflicts may arise where an individual:

a. has a financial interest in a bidding company;

b. has a family or close personal relationship with a bidder;

c. expects future employment or benefits from a supplier;

d. has received gifts, hospitality, or favors from a bidder;

e. has any other interest that could reasonably affect impartiality.

Failure to disclose procurement conflicts may result in disciplinary action and invalidation of the procurement process where appropriate.

7.10 Management Measures

Where a conflict of interest has been identified, ILA shall implement appropriate measures to protect the integrity of organizational decision-making.

Management measures may include:

a. requiring full disclosure of the conflict;

b. recording the conflict in the Register of Interests;

c. restricting access to confidential information;

d. recusal from discussions, evaluations, negotiations, or decision-making;

e. reassignment of duties or responsibilities;

f. enhanced supervision or independent review;

g. cancellation or modification of the affected transaction;

h. termination of contractual relationships where necessary;

i. disciplinary action for failure to disclose or manage conflicts appropriately.

The Executive Director, or where applicable the Board of Directors, shall determine the most appropriate management response based on the nature and seriousness of the conflict.

All conflict of interest management decisions shall be documented and retained in accordance with ILA's records management requirements.

ILA shall periodically review the effectiveness of its conflict of interest management framework to ensure continued compliance with legal obligations, donor expectations, and international standards of good governance.

CHAPTER EIGHT

GIFTS, HOSPITALITY, DONATIONS AND SPONSORSHIPS

8.1 Acceptable Gifts

Initiative for Legal Aid (ILA) recognizes that modest gifts and customary expressions of courtesy may arise during professional engagements. However, all gifts must never influence, or appear to influence, official decisions or compromise the independence, impartiality or integrity of the Organization.

Acceptable gifts shall:

a. be of nominal value and consistent with local cultural practice;

b. be openly given and transparently received;

c. not create actual or perceived obligations;

d. not influence procurement, recruitment, grant management or financial decisions;

e. comply with donor requirements and applicable laws;

f. be reported where required under this Policy.

Examples of acceptable gifts include:

- organizational souvenirs;
- plaques or certificates of appreciation;
- promotional materials of insignificant value;
- modest refreshments during official meetings.

Where there is uncertainty regarding the acceptability of any gift, employees shall seek written guidance before accepting it.

8.2 Prohibited Gifts

ILA strictly prohibits accepting, offering, requesting or giving gifts intended to influence decisions or obtain improper advantages.

Prohibited gifts include:

a. cash or cash equivalents;

b. gift cards or prepaid vouchers;

c. expensive personal items;

d. luxury travel unrelated to official duties;

e. personal loans;

f. personal discounts unavailable to the public;

g. gifts during procurement, recruitment or grant evaluation processes;

h. gifts from current or prospective suppliers intended to influence procurement;

i. gifts from beneficiaries seeking preferential treatment;

j. any gift prohibited by donor regulations or national law.

No employee shall solicit gifts from any stakeholder.

Employees must politely decline prohibited gifts and immediately report any attempt to provide such gifts.

8.3 Gift Register

ILA shall maintain a centralized Gift Register to promote transparency and accountability.

The register shall record:

a. date received;

b. recipient;

c. donor identity;

d. description of the gift;

e. estimated value;

f. reason for the gift;

g. approval decision;

h. final disposition of the gift.

The Finance and Administration Department shall maintain the Register.

The Executive Director shall periodically review all entries.

High-value gifts may become the property of ILA rather than the individual employee.

The Register shall be available for internal audit, donor review and Board oversight.

8.4 Hospitality

Hospitality may be accepted only where it serves legitimate organizational purposes.

Permissible hospitality includes:

a. working lunches;

b. official conferences;

c. donor meetings;

d. professional networking events;

e. ceremonial events.

Hospitality shall not:

- influence decision-making;
- compromise impartiality;
- create conflicts of interest;
- exceed reasonable limits;
- include lavish entertainment.

Employees shall not provide hospitality using organizational resources without proper authorization.

Where hospitality exceeds prescribed thresholds, prior written approval shall be obtained.

8.5 Travel Sponsorship

Travel funded by external organizations may only be accepted where it advances ILA's mission and does not compromise organizational independence.

Travel sponsorship shall:

a. have a legitimate official purpose;

b. receive prior written approval;

c. be transparently disclosed;

d. comply with donor conditions;

e. avoid conflicts of interest.

Travel funded by vendors currently participating in procurement processes is prohibited unless expressly authorized under exceptional circumstances.

All sponsored travel shall be documented.

8.6 Donations

ILA may receive donations that support its mission provided they are lawful, transparent and free from improper influence.

Before accepting donations, ILA shall assess:

a. donor identity;

b. source of funds;

c. legal compliance;

d. reputational risks;

e. donor conditions;

f. conflict of interest risks.

ILA shall reject donations that:

- originate from illegal activities;
- involve proceeds of corruption;
- undermine organizational independence;
- conflict with humanitarian principles;
- damage organizational reputation.

All donations shall be properly receipted, recorded and reported.

8.7 Charitable Contributions

ILA may make charitable contributions where such activities support humanitarian, educational or community development objectives consistent with its mandate.

Charitable contributions shall:

a. be approved in accordance with delegated authority;

b. be properly documented;

c. avoid political influence;

d. avoid personal benefit;

e. comply with donor restrictions;

f. be transparently reported.

No employee shall authorize charitable contributions for personal gain.

8.8 Political Contributions

ILA maintains strict political neutrality.

Organizational funds, assets, facilities or resources shall not be used to support:

a. political parties;

b. political candidates;

c. election campaigns;

d. partisan political activities;

e. political fundraising.

Employees acting in their personal capacities shall clearly distinguish personal political activities from official organizational responsibilities.

ILA shall not permit organizational branding or resources to be used for political purposes.

8.9 Approval Procedures

Approvals relating to gifts, hospitality, donations and sponsorships shall follow established delegation of authority.

Approval procedures shall include:

a. written disclosure;

b. value assessment;

c. conflict of interest review;

d. donor compliance review;

e. legal compliance review where necessary;

f. documented approval;

g. maintenance of supporting records.

The Executive Director may approve matters within delegated authority.

The Board of Directors shall approve significant transactions involving substantial value, strategic partnerships or matters presenting significant reputational risk.

Failure to obtain required approval constitutes a breach of this Policy and may result in disciplinary action.

CHAPTER NINE

WHISTLEBLOWING FRAMEWORK

9.1 Principles

Initiative for Legal Aid (ILA) recognizes that timely reporting of suspected fraud, corruption and other forms of misconduct is essential to safeguarding organizational resources, protecting beneficiaries, maintaining donor confidence and promoting a culture of integrity and accountability.

ILA is committed to fostering an environment in which employees, Board members, volunteers, consultants, interns, contractors, suppliers, beneficiaries and other stakeholders are encouraged to report genuine concerns without fear of retaliation, intimidation or victimization.

The Whistleblowing Framework is founded on the following principles:

a. integrity and honesty in reporting;

b. protection of whistleblowers acting in good faith;

c. confidentiality of disclosures;

d. impartiality and independence in handling reports;

e. fairness to all parties involved;

f. timely assessment and response;

g. accountability and transparency;

h. protection of evidence;

i. zero tolerance for retaliation;

j. compliance with applicable laws and donor requirements.

All reports shall be handled professionally, objectively and consistently.

9.2 Protected Disclosures

ILA shall protect individuals who disclose information that they reasonably believe demonstrates actual, suspected or attempted misconduct.

Protected disclosures include reports concerning:

a. fraud;

b. corruption;

c. bribery;

d. theft;

e. embezzlement;

f. procurement irregularities;

g. financial misconduct;

h. grant misuse;

i. abuse of authority;

j. conflicts of interest;

k. payroll fraud;

l. falsification of records;

m. cyber fraud;

n. money laundering;

o. retaliation against whistleblowers;

p. violations of this Policy or other organizational policies;

q. violations of applicable laws or donor regulations.

Protection applies regardless of whether the allegation is ultimately substantiated, provided the disclosure was made honestly and in good faith.

9.3 Anonymous Reporting

ILA recognizes that some individuals may fear retaliation and therefore allows anonymous reporting.

Anonymous reports shall:

a. be accepted through approved reporting mechanisms;

b. be assessed based on available evidence;

c. receive the same objective consideration as identified reports;

d. not be dismissed solely because the reporter is unidentified.

Although anonymity may limit the Organization's ability to obtain additional information, every reasonable effort shall be made to investigate credible anonymous allegations.

ILA shall not attempt to identify anonymous whistleblowers except where required by law.

9.4 Confidential Reporting

Where a whistleblower chooses to identify themselves, ILA shall maintain strict confidentiality to the fullest extent possible.

Confidential information shall only be disclosed where:

a. disclosure is required by law;

b. disclosure is necessary for a fair investigation;

c. disclosure is authorized by the whistleblower;

d. disclosure is required by a competent court or lawful authority.

Persons involved in receiving, investigating or managing reports shall maintain confidentiality throughout the reporting and investigation process.

Unauthorized disclosure of a whistleblower's identity constitutes serious misconduct and may result in disciplinary action.

9.5 Reporting Channels

ILA shall establish multiple secure reporting channels to encourage timely disclosure of suspected misconduct.

Reporting channels may include:

a. immediate supervisors;

b. departmental heads;

c. Executive Director;

d. Board Chairperson;

e. Internal Audit;

f. designated Ethics or Compliance Officer;

g. whistleblower hotline;

h. official whistleblowing email address;

i. secure complaint boxes;

j. authorized external reporting mechanisms.

Employees should ordinarily report concerns through internal channels unless circumstances make internal reporting inappropriate or unsafe.

All reports shall be acknowledged, recorded and assessed promptly.

9.6 Hotline

ILA may establish a confidential whistleblower hotline to facilitate secure reporting of suspected misconduct.

The hotline shall:

a. be accessible to employees and external stakeholders;

b. permit anonymous reporting where practicable;

c. maintain confidentiality;

d. record reports securely;

e. ensure prompt referral for assessment.

Only authorized personnel shall have access to hotline records.

Hotline records shall be retained in accordance with ILA's Records Management Policy and applicable legal requirements.

9.7 Email

ILA shall maintain a dedicated official email address for receiving whistleblower reports.

Reports submitted through email should, where possible, include:

a. nature of the allegation;

b. date of occurrence;

c. persons involved;

d. supporting documents or evidence;

e. names of witnesses, if available;

f. any immediate risks requiring urgent attention.

Electronic reports shall be securely stored and accessible only to authorized officers.

All electronic communications shall comply with ILA's ICT and Data Protection policies.

9.8 Complaint Boxes

ILA may establish secure complaint boxes at its offices and programme locations to facilitate confidential reporting.

Complaint boxes shall:

a. be placed in secure and accessible locations;

b. be regularly monitored by authorized personnel;

c. protect anonymity where desired;

d. be opened only by designated officials;

e. maintain confidentiality throughout the review process.

Records of complaints received through complaint boxes shall be entered into the organizational case management system for appropriate follow-up.

9.9 External Reporting

ILA encourages internal reporting as the primary mechanism for addressing misconduct. However, external reporting may be appropriate where:

a. internal reporting is unsafe;

b. there is a reasonable belief that evidence may be concealed or destroyed;

c. senior management is implicated;

d. the matter involves criminal conduct;

e. donor agreements require external notification;

f. reporting to competent public authorities is legally required.

External reporting may be made to:

- law enforcement agencies;
- anti-corruption institutions;
- regulatory authorities;
- donor agencies;
- competent courts or tribunals;
- other legally authorized oversight bodies.

Individuals making external disclosures shall act responsibly, honestly and in accordance with applicable law.

9.10 Emergency Reporting

Certain incidents require immediate reporting due to their seriousness or potential impact on the Organization, beneficiaries, staff or public interest.

Emergency reporting applies to situations involving:

a. significant financial loss;

b. ongoing theft or fraud;

c. destruction or concealment of evidence;

d. imminent threats to life or safety;

e. major cyber security incidents;

f. suspected terrorist financing or money laundering;

g. serious corruption involving senior officials;

h. substantial donor fund diversion;

i. any incident posing immediate reputational or operational risk to ILA.

Emergency reports shall receive immediate attention and may require urgent protective measures, including:

- securing evidence;
- suspension of transactions;
- protection of affected persons;
- notification of senior management;
- activation of crisis management procedures;
- referral to law enforcement where appropriate.

No employee shall delay reporting an emergency incident due to uncertainty regarding its ultimate validity. Reports made honestly and in good faith shall receive protection under this Policy.

CHAPTER TEN

WHISTLEBLOWER PROTECTION

10.1 Confidentiality

Initiative for Legal Aid (ILA) is committed to protecting the identity and privacy of whistleblowers to encourage the reporting of suspected fraud, corruption, unethical conduct and other forms of misconduct. Confidentiality is fundamental to maintaining trust in the whistleblowing process and ensuring that individuals can report concerns without fear of exposure.

ILA shall ensure that:

a. the identity of a whistleblower is treated as strictly confidential;

b. information relating to a disclosure is shared only with persons who have a legitimate need to know;

c. records relating to whistleblower reports are securely maintained and protected from unauthorized access;

d. confidential information is disclosed only where required by law, court order or with the informed consent of the whistleblower;

e. all persons involved in receiving, assessing and investigating reports are bound by confidentiality obligations.

Employees, Board members, consultants, volunteers and contractors who unlawfully disclose confidential whistleblower information shall be subject to disciplinary action and, where applicable, legal proceedings.

Confidentiality obligations shall continue even after an investigation has concluded.

10.2 Protection Against Retaliation

ILA adopts a zero-tolerance approach to retaliation against any individual who makes a protected disclosure or participates in an investigation in good faith.

Retaliation includes any adverse action taken because a person has reported or assisted in reporting suspected misconduct.

Prohibited retaliatory actions include:

a. dismissal or termination of employment;

b. demotion or denial of promotion;

c. reduction of salary or benefits;

d. harassment or intimidation;

e. discrimination or victimization;

f. unfair performance evaluations;

g. reassignment intended as punishment;

h. threats or coercion;

i. denial of training or professional opportunities;

j. blacklisting or reputational harm;

k. any other adverse employment or contractual action.

Any person found to have engaged in retaliation shall face appropriate disciplinary measures, which may include termination of employment, contractual sanctions or referral to law enforcement where criminal conduct is involved.

ILA shall investigate allegations of retaliation promptly and impartially and shall take immediate corrective action where retaliation is substantiated.

10.3 Witness Protection

Individuals who provide information, testimony or evidence during fraud investigations play a critical role in maintaining organizational accountability and shall receive appropriate protection.

ILA shall ensure that witnesses:

a. are treated with dignity, fairness and respect;

b. are protected from intimidation, harassment or coercion;

c. are not subjected to retaliation for cooperating with investigations;

d. have access to confidential reporting mechanisms if they experience threats or retaliation;

e. receive appropriate guidance regarding investigation procedures.

Witness protection measures shall be proportionate to the level of risk and may include adjustments to reporting lines, temporary workplace arrangements or other reasonable administrative measures necessary to safeguard their welfare.

10.4 Protection of Evidence

The preservation of evidence is essential to ensuring fair, objective and credible investigations.

Upon receiving a report of suspected misconduct, ILA shall take reasonable measures to protect relevant evidence from alteration, destruction, concealment or unauthorized access.

Protective measures may include:

a. securing physical documents;

b. preserving electronic records;

c. restricting access to sensitive information;

d. maintaining audit trails for digital evidence;

e. safeguarding financial and procurement records;

f. securing organizational assets connected to the allegation.

Employees shall not destroy, alter, conceal or falsify evidence relating to an investigation.

Any deliberate interference with evidence constitutes serious misconduct and may result in disciplinary action, civil recovery and criminal referral where appropriate.

10.5 Psychological Support

ILA recognizes that whistleblowers and witnesses may experience stress, anxiety or emotional distress arising from the reporting process or participation in investigations.

Where reasonably practicable, ILA shall provide appropriate support, which may include:

a. confidential counselling services;

b. access to employee assistance programmes, where available;

c. referrals to qualified psychosocial support providers;

d. reasonable workplace accommodations where necessary;

e. regular communication regarding the progress of the matter, where appropriate.

The provision of psychological support shall respect confidentiality and shall not compromise the independence or integrity of any investigation.

10.6 Remedies

Where a whistleblower or witness suffers retaliation or other adverse consequences as a result of making a protected disclosure in good faith, ILA shall take reasonable steps to restore the individual to the position they would have been in had the retaliation not occurred.

Available remedies may include:

a. reinstatement to employment or position;

b. restoration of salary, benefits or employment rights;

c. removal of disciplinary measures imposed in retaliation;

d. correction of personnel records;

e. reassignment where appropriate and agreed;

f. formal apology or acknowledgement of wrongdoing;

g. referral to competent authorities where legal remedies are available.

Nothing in this Policy limits any statutory or contractual rights available to whistleblowers under applicable law.

10.7 False Reports

ILA encourages responsible reporting and expects all disclosures to be made honestly and in good faith.

Knowingly making false, malicious or misleading allegations is prohibited.

A report shall be considered false where an individual deliberately provides fabricated information or intentionally makes allegations that they know to be untrue.

Persons who knowingly submit false reports may be subject to:

a. disciplinary action;

b. termination of employment or contractual relationship;

c. recovery of losses resulting from malicious allegations;

d. referral to law enforcement where criminal offences are committed.

The inability to substantiate an allegation following investigation shall not, by itself, constitute a false report.

No action shall be taken against a whistleblower solely because an allegation is not proven, provided the report was made honestly and in good faith.

10.8 Good Faith Reports

ILA strongly encourages all individuals to report concerns honestly, responsibly and with reasonable grounds for believing that the information disclosed is true.

A report is made in good faith where the whistleblower:

a. genuinely believes that misconduct has occurred, is occurring or is likely to occur;

b. does not act with malicious intent or personal vendetta;

c. provides information honestly and to the best of their knowledge;

d. cooperates with any subsequent inquiry or investigation where appropriate.

Whistleblowers acting in good faith shall receive the protections provided under this Policy even if investigations ultimately conclude that no misconduct occurred.

ILA shall promote a culture in which raising genuine concerns is regarded as an important contribution to good governance, accountability and organizational integrity rather than an act of disloyalty.

CHAPTER ELEVEN

INVESTIGATION MANAGEMENT

11.1 Investigation Principles

Initiative for Legal Aid (ILA) is committed to ensuring that all allegations of fraud, corruption, financial misconduct and related offences are investigated promptly, independently, professionally and fairly. Effective investigations are essential to protecting organizational resources, ensuring accountability, strengthening internal controls and maintaining the confidence of beneficiaries, donors, partners and the public.

All investigations conducted under this Policy shall be guided by the following principles:

a. independence and impartiality;

b. legality and compliance with applicable laws;

c. fairness and procedural justice;

d. confidentiality and protection of sensitive information;

e. objectivity and evidence-based decision-making;

f. timeliness and efficiency;

g. integrity and professionalism;

h. protection of whistleblowers and witnesses;

i. respect for the rights and dignity of all persons involved;

j. accountability throughout the investigative process.

Investigations shall seek to establish facts rather than assign blame prematurely and shall be conducted without bias or undue influence.

11.2 Case Assessment

Upon receipt of a report or allegation, ILA shall undertake an initial case assessment to determine whether a formal investigation is warranted.

The assessment shall consider:

a. the nature and seriousness of the allegation;

b. the credibility and reliability of the information provided;

c. the potential financial, operational, legal or reputational impact;

d. whether sufficient preliminary information exists to proceed;

e. immediate risks requiring urgent intervention;

f. possible conflicts of interest affecting the assessment process;

g. applicable donor, contractual or statutory reporting obligations.

Based on the assessment, the Organization may:

- close the matter where the allegation is clearly unfounded;
- request additional information;
- refer the matter to another internal process;
- initiate a formal investigation;
- refer the matter to law enforcement or other competent authorities where appropriate.

The outcome of the assessment shall be documented and retained in the case file.

11.3 Investigation Planning

Where a formal investigation is approved, an investigation plan shall be developed before substantive investigative activities commence.

The investigation plan shall, where appropriate, include:

a. objectives of the investigation;

b. scope of the investigation;

c. issues to be examined;

d. applicable laws, policies and donor requirements;

e. investigators assigned;

f. anticipated timelines;

g. required resources;

h. evidence collection strategy;

i. witness identification;

j. risk assessment and mitigation measures.

The investigation plan may be revised where new information emerges during the investigation.

Investigators shall ensure that investigative activities remain proportionate to the seriousness and complexity of the allegation.

11.4 Collection of Evidence

Evidence shall be collected lawfully, objectively and systematically to establish relevant facts.

Evidence may include:

a. financial records;

b. accounting documents;

c. procurement files;

d. contracts and agreements;

e. correspondence;

f. emails and electronic communications;

g. bank records;

h. payroll records;

i. inventory records;

j. photographs, videos and audio recordings;

k. witness statements;

l. physical evidence.

Investigators shall ensure that:

- evidence is authentic and reliable;
- proper chain of custody is maintained;
- evidence is preserved against loss, alteration or destruction;
- all relevant evidence, including exculpatory evidence, is considered.

Evidence obtained unlawfully shall not be relied upon where doing so would violate applicable law or compromise the integrity of the investigation.

11.5 Digital Evidence

ILA recognizes that digital information is increasingly central to fraud investigations.

Digital evidence may include:

a. emails;

b. electronic documents;

c. accounting software records;

d. system audit logs;

e. cloud-based records;

f. mobile device data;

g. CCTV recordings;

h. internet usage records;

i. digital photographs;

j. electronic payment records.

Digital evidence shall:

- be collected using appropriate forensic methods where necessary;
- maintain data integrity throughout the investigation;
- preserve metadata wherever practicable;
- comply with applicable data protection and privacy laws;
- be securely stored and protected from unauthorized access.

Only authorized personnel shall access or analyze sensitive electronic evidence.

11.6 Interviews

Interviews are an essential investigative tool and shall be conducted fairly, respectfully and professionally.

Interviews may be conducted with:

a. complainants;

b. whistleblowers;

c. witnesses;

d. suspects;

e. subject matter experts;

f. contractors or suppliers;

g. beneficiaries or partners, where relevant.

Investigators shall:

- clearly explain the purpose of the interview;
- maintain neutrality throughout questioning;
- avoid intimidation, coercion or harassment;
- accurately document responses;
- provide interviewees with an opportunity to clarify or correct statements where appropriate.

Interview records shall be securely maintained as part of the investigation file.

11.7 Investigation Reports

At the conclusion of every investigation, a written investigation report shall be prepared.

The report shall, where applicable, include:

a. background of the allegation;

b. investigation objectives;

c. scope of the investigation;

d. methodology used;

e. evidence reviewed;

f. factual findings;

g. analysis of evidence;

h. conclusions;

i. recommendations;

j. proposed corrective or disciplinary actions;

k. recommendations for control improvements;

l. referral recommendations where criminal conduct is suspected.

Investigation reports shall be factual, objective and supported by sufficient evidence.

Reports shall avoid speculation and clearly distinguish established facts from opinions.

11.8 Investigation Standards

Investigations undertaken by ILA shall comply with recognized principles of professional investigation and good governance.

Investigators shall:

a. act independently and objectively;

b. avoid conflicts of interest;

c. maintain confidentiality;

d. exercise due professional care;

e. respect legal and procedural rights;

f. maintain complete documentation;

g. comply with applicable donor standards and organizational policies.

Where specialized expertise is required, ILA may engage qualified external investigators, auditors, forensic specialists or legal experts.

All investigations shall adhere to the highest standards of integrity and professionalism.

11.9 Quality Assurance

ILA shall establish quality assurance mechanisms to ensure consistency, reliability and continuous improvement in investigations.

Quality assurance measures may include:

a. supervisory review of investigation plans;

b. review of evidence management procedures;

c. verification of factual findings;

d. legal review where necessary;

e. compliance review against organizational policies;

f. periodic evaluation of investigation performance;

g. lessons learned reviews following significant cases.

Recommendations arising from quality assurance reviews shall be used to strengthen future investigations, internal controls and fraud prevention measures.

11.10 Case Closure

A case shall be formally closed only after all necessary investigative activities have been completed and appropriate decisions have been made.

Case closure shall include:

a. confirmation that investigation objectives have been achieved;

b. documentation of findings and conclusions;

c. implementation or referral of disciplinary, administrative, civil or criminal actions where appropriate;

d. communication of outcomes to relevant authorities on a need-to-know basis;

e. secure archiving of investigation records;

f. recording lessons learned and recommendations for organizational improvement.

Where new and credible evidence emerges after closure, the Executive Director or other authorized authority may approve the reopening of the investigation.

Closed case records shall be retained in accordance with ILA's Records Management Policy, Data Protection Policy, donor requirements and applicable legal retention obligations.

CHAPTER TWELVE

DISCIPLINARY, ADMINISTRATIVE AND LEGAL ACTION

12.1 Disciplinary Measures

Initiative for Legal Aid (ILA) shall take appropriate disciplinary action against any employee, volunteer, intern, consultant or other individual under its authority who is found, following due process, to have engaged in fraud, corruption, bribery, theft or any other prohibited conduct under this Policy.

Disciplinary measures are intended to:

a. uphold the integrity of the Organization;

b. deter misconduct;

c. promote accountability;

d. protect organizational resources and reputation;

e. reinforce compliance with applicable laws, donor requirements and organizational policies.

Disciplinary action shall be guided by the principles of:

- fairness;
- proportionality;
- consistency;
- impartiality;
- due process;
- confidentiality.

Depending on the seriousness of the misconduct, disciplinary measures may include:

a. verbal warning;

b. written warning;

c. mandatory training or counselling;

d. suspension pending investigation;

e. suspension without pay where permitted by law;

f. demotion or reassignment;

g. withholding of benefits where legally permissible;

h. termination of employment or contractual engagement;

i. any other lawful disciplinary sanction provided under ILA's Human Resources Policies.

No disciplinary action shall be imposed without providing the affected individual with an opportunity to respond to the allegations, except where immediate action is authorized by law or organizational policy to protect organizational interests.

12.2 Administrative Measures

In addition to disciplinary sanctions, ILA may impose administrative measures to protect the Organization, preserve evidence, reduce operational risks and strengthen internal controls.

Administrative measures may include:

a. temporary reassignment of duties;

b. restriction of system access;

c. suspension of financial approval authority;

d. removal from procurement committees;

e. suspension of delegated authority;

f. increased supervision;

g. mandatory declaration of conflicts of interest;

h. additional financial or operational oversight;

i. withdrawal of access to organizational assets or facilities.

Administrative measures may be implemented before, during or after an investigation where necessary to safeguard organizational interests and shall not be interpreted as a determination of guilt.

12.3 Contractual Remedies

ILA reserves the right to exercise contractual remedies against contractors, consultants, suppliers, service providers, implementing partners, vendors and other third parties who engage in fraud, corruption or other prohibited conduct.

Available contractual remedies may include:

a. termination of contracts;

b. suspension of contractual performance;

c. withholding of payments;

d. recovery of overpayments;

e. rejection of goods or services;

f. cancellation of procurement awards;

g. enforcement of contractual indemnities;

h. recovery of contractual damages;

i. invocation of performance guarantees or security bonds.

Contractual remedies shall be exercised in accordance with the relevant contract terms, procurement policies and applicable law.

12.4 Civil Recovery

Where ILA suffers financial loss, property loss or other measurable damage arising from fraud or misconduct, the Organization shall take reasonable steps to recover its losses through civil or administrative processes.

Civil recovery may include:

a. recovery of stolen funds;

b. compensation for financial losses;

c. restitution of organizational assets;

d. recovery of interest where applicable;

e. damages arising from contractual breaches;

f. enforcement of court judgments;

g. negotiated settlement agreements where appropriate.

The decision to pursue civil recovery shall consider:

- the amount involved;
- likelihood of recovery;
- legal costs;
- available evidence;
- donor expectations;
- organizational interests.

Civil recovery may proceed independently of disciplinary or criminal proceedings

12.5 Criminal Referral

Where investigations indicate that criminal offences may have been committed, ILA shall refer the matter to the appropriate law enforcement or prosecutorial authorities in accordance with applicable laws.

Criminal referral may be appropriate for offences including:

a. fraud;

b. corruption;

c. bribery;

d. theft;

e. embezzlement;

f. forgery;

g. money laundering;

h. cybercrime;

i. identity theft;

j. obstruction of justice;

k. destruction of evidence;

l. other criminal offences.

ILA shall cooperate fully with competent authorities by providing relevant information, documentation and lawful assistance while safeguarding confidentiality and legal rights.

Referral for criminal investigation shall not prevent ILA from pursuing disciplinary, contractual or civil remedies.

12.6 Recovery of Assets

ILA shall take all reasonable and lawful measures to recover assets that have been lost, stolen, misappropriated or unlawfully obtained through fraud or other misconduct.

Asset recovery measures may include:

a. recovery of cash and bank balances;

b. repossession of equipment and vehicles;

c. recovery of inventory and supplies;

d. recovery of electronic devices;

e. freezing or securing assets where legally permissible;

f. recovery through insurance claims;

g. enforcement of court orders;

h. negotiated voluntary restitution.

Recovered assets shall be properly documented, recorded in the accounting records and returned to the appropriate organizational asset registers.

The Finance Department shall ensure that recovered funds are accurately reflected in the financial records.

12.7 Debarment

ILA may suspend or debar individuals or organizations from participating in its activities where they have engaged in fraud, corruption or other serious misconduct.

Debarment may apply to:

a. suppliers;

b. contractors;

c. consultants;

d. implementing partners;

e. service providers;

f. volunteers;

g. grant recipients;

h. other third parties.

Grounds for debarment may include:

- fraudulent practices;
- corrupt practices;
- collusion;
- coercion;
- obstruction of investigations;
- repeated contractual breaches;
- serious ethical misconduct.

Debarment may be temporary or permanent depending on the seriousness of the misconduct.

Before debarment is imposed, affected parties shall, where appropriate, be afforded an opportunity to respond in accordance with principles of procedural fairness.

ILA may share debarment information with donors, regulators or other authorized entities where permitted by law, contractual obligations or donor requirements.

12.8 Donor Notification

ILA recognizes its obligation to maintain transparency and accountability in its relationships with donors.

Where fraud, corruption or other serious misconduct affects donor-funded resources or contractual obligations, ILA shall notify the affected donor(s) in accordance with:

a. applicable grant agreements;

b. donor reporting requirements;

c. contractual obligations;

d. applicable laws;

e. organizational policies.

Donor notifications shall, where appropriate, include:

- the nature of the incident;
- preliminary assessment of the impact;
- actions taken to secure assets and evidence;
- status of the investigation;
- corrective measures implemented;
- recovery efforts;
- planned preventive actions.

Notifications shall be made promptly while ensuring that ongoing investigations are not compromised and that confidentiality obligations are respected.

The Executive Director shall be responsible for ensuring timely donor communication, unless the Board of Directors determines that another authorized officer should perform this function due to the nature of the matter.

CHAPTER THIRTEEN

FRAUD RESPONSE AND INCIDENT MANAGEMENT

13.1 Incident Response

Initiative for Legal Aid (ILA) shall maintain a structured and coordinated approach to responding to actual, suspected or attempted fraud, corruption and other forms of financial or administrative misconduct. An effective incident response framework enables the Organization to minimize financial losses, protect beneficiaries and staff, preserve evidence, maintain donor confidence and ensure compliance with legal and contractual obligations.

The objectives of fraud incident response are to:

a. promptly contain and manage suspected fraud incidents;

b. protect organizational assets, information and resources;

c. preserve evidence for administrative, civil or criminal proceedings;

d. safeguard the rights of affected individuals;

e. minimize operational disruption;

f. ensure timely reporting to appropriate authorities and donors where required;

g. support fair and objective investigations;

h. strengthen organizational controls to prevent recurrence.

Every employee, volunteer, consultant, contractor and Board member has a responsibility to report suspected fraud immediately upon becoming aware of it.

ILA shall respond to all reported incidents proportionately, objectively and without undue delay.

13.2 Immediate Actions

Upon receiving information regarding suspected fraud or misconduct, ILA shall undertake immediate actions necessary to contain risks and prevent further loss or damage.

Immediate actions may include:

a. securing the location of the incident;

b. protecting financial resources and organizational assets;

c. suspending questionable transactions where appropriate;

d. restricting access to financial systems, records or premises;

e. safeguarding electronic systems and digital data;

f. notifying designated management officials;

g. initiating preliminary risk assessment;

h. documenting the incident;

i. activating the investigation process where appropriate.

Emergency protective measures shall be implemented without prejudice to the rights of individuals who may later be found not to have engaged in misconduct.

Actions taken shall be proportionate to the seriousness and urgency of the incident.

13.3 Preservation of Evidence

Preserving evidence is essential to ensuring the integrity of investigations and any subsequent disciplinary, civil or criminal proceedings.

Immediately following the identification of a suspected fraud incident, ILA shall take reasonable measures to preserve all relevant evidence.

Evidence preservation shall include:

a. securing physical documents;

b. preserving accounting records;

c. protecting procurement files;

d. retaining electronic records and audit logs;

e. safeguarding emails and digital communications;

f. securing electronic devices where appropriate;

g. documenting the chain of custody for evidence;

h. preventing unauthorized access, alteration or destruction of records.

Employees shall not remove, destroy, conceal, falsify or interfere with any evidence related to a suspected incident.

Any intentional destruction or concealment of evidence shall constitute serious misconduct and may result in disciplinary action and referral to competent authorities.

13.4 Crisis Management

Certain fraud incidents may significantly affect ILA's operations, financial stability, reputation or relationships with donors and beneficiaries. In such circumstances, the Organization shall activate appropriate crisis management measures.

A fraud incident may be treated as a crisis where it:

a. involves substantial financial loss;

b. affects multiple programmes or projects;

c. compromises donor-funded resources;

d. threatens organizational continuity;

e. attracts significant public or media attention;

f. involves senior management or governance bodies;

g. creates serious legal or regulatory risks;

h. affects the safety or wellbeing of staff or beneficiaries.

Where necessary, the Executive Director may establish a Crisis Management Team to coordinate organizational responses.

The Crisis Management Team may include representatives from:

- Executive Management;
- Finance;
- Human Resources;

- Internal Audit;
- Legal Services;
- ICT;
- Communications;
- Programme Management;
- other technical personnel as required.

The Team shall coordinate response activities, monitor developments, provide strategic guidance and ensure continuity of essential operations.

13.5 Communication

Effective communication is essential during fraud incidents to maintain transparency while protecting investigations and confidential information.

ILA shall ensure that communications relating to fraud incidents are:

a. accurate;

b. timely;

c. consistent;

d. confidential where required;

e. authorized through appropriate management channels.

Communication may involve:

- employees;
- the Board of Directors;
- donors;
- implementing partners;
- beneficiaries where appropriate;
- auditors;
- regulators;
- law enforcement agencies;
- insurance providers;
- the public or media where necessary.

Only authorized spokespersons shall issue public statements regarding fraud incidents.

No employee shall disclose confidential investigation information without proper authorization.

Communications shall balance transparency with the need to protect investigations, legal proceedings and the rights of affected individuals.

13.6 Recovery

Following the resolution of a fraud incident, ILA shall take all reasonable steps to recover losses and restore normal operations.

Recovery efforts may include:

a. recovery of stolen or misappropriated funds;

b. recovery of organizational assets;

c. enforcement of contractual remedies;

d. insurance claims;

e. civil recovery proceedings;

f. implementation of disciplinary actions;

g. strengthening internal controls;

h. restoration of information systems;

i. updating financial and asset records.

Recovery activities shall also focus on restoring stakeholder confidence and improving organizational resilience.

Where donor-funded resources are affected, recovery efforts shall be undertaken in accordance with applicable donor agreements and reporting obligations.

13.7 Lessons Learned

ILA recognizes that every fraud incident provides valuable opportunities for organizational learning and continuous improvement.

Upon closure of significant fraud cases, the Organization shall conduct a lessons learned review to identify:

a. root causes of the incident;

b. weaknesses in internal controls;

c. gaps in policies or procedures;

d. training needs;

e. governance weaknesses;

f. procurement or financial control deficiencies;

g. opportunities for strengthening fraud prevention.

Lessons learned shall be used to:

- revise policies and procedures;
- improve fraud risk assessments;
- strengthen internal controls;
- enhance staff awareness and training;
- improve investigation practices;
- reinforce accountability mechanisms;
- inform future organizational planning.

Management shall monitor the implementation of agreed corrective actions and periodically report progress to the Board of Directors and, where applicable, donors.

ILA is committed to fostering a culture of continuous learning in which fraud incidents are systematically analysed to improve governance, accountability and organizational effectiveness.

CHAPTER FOURTEEN

INTERNAL CONTROLS AND FRAUD PREVENTION SYSTEMS

14.1 Internal Controls

The Initiative for Legal Aid (ILA) recognizes that effective internal controls are the cornerstone of fraud prevention, accountability, transparency, and sound organizational governance. Internal controls provide reasonable assurance that organizational objectives are achieved, resources are safeguarded, financial information is reliable, laws and donor requirements are complied with, and fraud risks are minimized.

ILA shall establish, maintain and continuously improve a comprehensive system of preventive, detective and corrective internal controls across all organizational functions.

The internal control system shall be guided by the principles of:

a. accountability;

b. transparency;

c. segregation of duties;

d. authorization and approval;

e. documentation and record keeping;

f. supervision and monitoring;

g. independent verification;

h. proportionality of controls to risk; and

i. continuous improvement.

Management shall regularly review the effectiveness of internal controls and ensure that identified weaknesses are promptly addressed.

14.2 Financial Controls

ILA shall maintain strong financial controls to protect cash, bank accounts, grants, donations and all financial resources from fraud, theft, abuse or misuse.

Financial controls shall include, but not be limited to:

a. approved annual budgets for all programmes and operations;

b. segregation of responsibilities for authorization, payment processing, recording and reconciliation;

c. dual signatory requirements for bank transactions;

d. independent review and approval of all expenditures;

e. monthly bank reconciliations;

f. regular cash counts;

g. controlled access to accounting systems;

h. periodic financial reporting;

i. supporting documentation for every transaction;

j. expenditure verification before payment;

k. donor budget compliance reviews;

l. independent internal and external audits.

No employee shall authorize, process and approve the same financial transaction.

14.3 Procurement Controls

Procurement activities present significant fraud risks and therefore require enhanced controls throughout the procurement cycle.

ILA shall ensure that procurement processes are conducted in accordance with the Procurement and Asset Management Policy and applicable donor regulations.

Controls shall include:

a. approved procurement plans;

b. competitive bidding procedures;

c. transparent evaluation processes;

d. documented bid evaluations;

e. conflict of interest declarations;

f. supplier due diligence;

g. segregation between requesting, approving and receiving officers;

h. contract approval procedures;

i. inspection and acceptance of goods before payment;

j. procurement file documentation;

k. periodic supplier performance reviews; and

l. procurement audits.

Any attempt to manipulate procurement procedures shall constitute serious misconduct.

14.4 Asset Controls

ILA shall establish effective controls to safeguard all organizational assets against theft, misuse, damage or unauthorized disposal.

Assets include, but are not limited to:

a. cash;

b. vehicles;

c. office equipment;

d. computers;

e. furniture;

f. mobile devices;

g. legal reference materials;

h. project equipment;

i. inventories; and

j. donor-funded assets.

Control measures shall include:

a. comprehensive asset registers;

b. unique asset identification numbers;

c. periodic physical verification;

d. controlled asset movement procedures;

e. authorized disposal processes;

f. maintenance schedules;

g. secure storage facilities;

h. insurance where appropriate;

i. custody records; and

j. annual asset reconciliation.

Employees entrusted with organizational assets shall remain personally accountable for their proper use and safekeeping.

14.5 Payroll Controls

Payroll systems shall incorporate adequate safeguards to prevent payroll fraud, unauthorized payments and manipulation of employee records.

Payroll controls shall include:

a. maintenance of an approved staff establishment;

b. verification of employee identity;

c. documented employment contracts;

d. segregation of payroll preparation and approval functions;

e. independent payroll review;

f. monthly payroll reconciliation;

g. removal of terminated employees without delay;

h. verification of attendance records where applicable;

i. secure payroll databases;

j. restricted access to payroll information;

k. periodic payroll audits; and

l. management approval before salary payments.

Ghost employees, unauthorized salary adjustments or fictitious allowances are strictly prohibited.

14.6 ICT Controls

ILA recognizes that information technology systems are increasingly vulnerable to cyber fraud and unauthorized access.

The organization shall establish appropriate ICT security controls to protect information systems, electronic records and digital assets.

ICT controls shall include:

a. user authentication procedures;

b. strong password requirements;

c. multi-factor authentication where feasible;

d. controlled user access rights;

e. regular software updates;

f. antivirus and malware protection;

g. firewall protection;

h. encrypted storage of sensitive information;

i. secure electronic backups;

j. disaster recovery procedures;

k. monitoring of system activities;

l. cyber incident response procedures;

m. secure disposal of electronic media; and

n. periodic ICT security assessments.

Unauthorized access to organizational information systems constitutes serious misconduct and may result in disciplinary and legal action.

14.7 Access Controls

Access to organizational facilities, information, financial systems and sensitive records shall be restricted according to official responsibilities and the principle of least privilege.

ILA shall ensure that:

a. only authorized personnel access restricted areas;

b. electronic access permissions are role-based;

c. visitor access is controlled and recorded;

d. confidential files are securely stored;

e. keys, access cards and passwords are properly managed;

f. terminated employees immediately lose system access;

g. access rights are periodically reviewed;

h. temporary access is documented and monitored;

i. confidential information is shared strictly on a need-to-know basis; and

j. unauthorized duplication or removal of organizational records is prohibited.

Managers shall periodically verify that access privileges remain appropriate for each employee.

14.8 Audit Trails

ILA shall maintain comprehensive audit trails to support accountability, investigations and fraud detection.

Audit trails shall provide a reliable record of organizational activities and enable the reconstruction of transactions where necessary.

Audit trails shall include:

a. financial transaction logs;

b. procurement documentation;

c. payroll records;

d. electronic system logs;

e. access logs;

f. approval records;

g. contract documentation;

h. inventory movement records;

i. grant expenditure records;

j. email and electronic communication records where legally permissible;

k. investigation records; and

l. management approval histories.

Audit trail records shall be protected from alteration, unauthorized deletion or destruction.

The Internal Auditor, external auditors, investigators and authorized oversight bodies shall have access to audit trail information in accordance with applicable laws, donor requirements and organizational policies.

Management shall regularly review audit trail information to identify unusual transactions, control weaknesses, emerging fraud risks and opportunities for strengthening internal controls.

CHAPTER FIFTEEN

RECORDS MANAGEMENT, CONFIDENTIALITY AND DATA PROTECTION

15.1 Confidential Records

The Initiative for Legal Aid (ILA) recognizes that effective records management and the protection of confidential information are essential to maintaining organizational integrity, protecting the rights of individuals, ensuring accountability, and supporting fraud prevention and investigation processes. Records relating to fraud, corruption, whistleblowing, investigations, disciplinary proceedings, and legal actions often contain sensitive personal and organizational information requiring the highest standards of confidentiality.

ILA shall establish and maintain secure systems for the creation, storage, management, use, sharing, archiving, and disposal of all records generated under this Policy.

Confidential records shall include, but not be limited to:

a. whistleblower reports;

b. investigation files;

c. disciplinary records;

d. audit reports;

e. financial records;

f. procurement documentation;

g. conflict of interest declarations;

h. witness statements;

i. legal opinions;

j. personnel records relating to misconduct;

k. digital evidence; and

l. correspondence concerning suspected fraud or corruption.

All confidential records shall be clearly identified, securely maintained, and accessed only by authorized persons performing official duties.

Unauthorized disclosure, copying, alteration, removal, or destruction of confidential records is strictly prohibited and may result in disciplinary, civil, or criminal action.

15.2 Case Files

ILA shall maintain complete, accurate, and well-organized case files for every fraud allegation, whistleblower report, investigation, disciplinary proceeding, recovery action, and legal referral.

Each case file shall, where applicable, contain:

a. the original complaint or report;

b. acknowledgement of receipt;

c. preliminary assessment documentation;

d. investigation plan;

e. evidence collected;

f. witness statements;

g. interview records;

h. financial analyses;

i. correspondence relating to the case;

j. investigation findings;

k. management decisions;

l. disciplinary actions taken;

m. recovery measures;

n. legal proceedings;

o. case closure report; and

p. lessons learned.

Case files shall be assigned unique reference numbers to facilitate tracking, monitoring, reporting, and retrieval.

No document shall be removed from a case file without proper authorization and documentation.

15.3 Digital Records

ILA recognizes the increasing reliance on electronic information systems in organizational operations and investigations. Digital records shall receive the same level of protection as physical records.

Digital records shall include:

a. electronic documents;

b. emails;

c. accounting system records;

d. procurement databases;

e. payroll records;

f. scanned documents;

g. electronic contracts;

h. digital photographs;

i. audio recordings;

j. video recordings;

k. electronic correspondence;

l. system-generated reports; and

m. electronic evidence obtained during investigations.

ILA shall ensure that digital records are:

a. securely stored;

b. regularly backed up;

c. protected against unauthorized access;

d. protected from alteration or deletion;

e. recoverable following system failures;

f. encrypted where appropriate;

g. retained in accordance with organizational retention schedules; and

h. monitored through appropriate audit logs.

Electronic records shall be admissible for investigative, disciplinary, administrative, and legal purposes where permitted by applicable law.

15.4 Access Control

Access to records governed by this Policy shall be restricted to authorized personnel based on official responsibilities and the principle of least privilege.

ILA shall establish access control procedures that ensure:

a. confidential records are available only to authorized persons;

b. investigation files are accessed solely by designated investigators and authorized management;

c. electronic systems require secure authentication;

d. physical records are stored in locked cabinets or secure archives;

e. visitor access to confidential records is prohibited unless formally authorized;

f. access rights are periodically reviewed;

g. access logs are maintained for sensitive electronic records;

h. terminated personnel immediately lose access privileges;

i. temporary access is documented and approved; and

j. unauthorized duplication or distribution of confidential information is prohibited.

Managers responsible for confidential information shall regularly verify that access permissions remain appropriate.

15.5 Record Retention

ILA shall retain records for periods that comply with applicable laws, donor requirements, contractual obligations, audit standards, and organizational policies.

Record retention periods shall take into account:

a. statutory legal requirements;

b. donor regulations;

c. ongoing investigations;

d. litigation holds;

e. audit requirements;

f. contractual obligations;

g. financial reporting obligations;

h. employment regulations; and

i. organizational operational needs.

Where litigation, criminal proceedings, disciplinary action, or investigations are pending, relevant records shall not be destroyed regardless of the normal retention schedule.

The Executive Director, in consultation with the Finance Manager, Human Resources Manager, Internal Auditor, and Legal Officer, shall ensure compliance with approved records retention schedules.

15.6 Secure Disposal

Records shall only be disposed of after the applicable retention period has expired and where no legal, contractual, investigative, or donor requirement requires their continued preservation.

Secure disposal methods shall include:

a. shredding of paper documents;

b. secure destruction of electronic storage devices;

c. permanent deletion of electronic files using approved methods;

d. destruction of backup media where appropriate;

e. supervised disposal procedures;

f. documentation of disposal activities; and

g. approval by designated management before destruction.

Records relating to fraud investigations, litigation, disciplinary proceedings, donor-funded projects, or criminal investigations shall not be destroyed without written authorization from the Executive Director and confirmation that no legal or operational requirement necessitates their retention.

Improper destruction of records shall constitute serious misconduct.

15.7 Data Protection

ILA is committed to protecting personal data and confidential information collected, processed, stored, and shared in the implementation of this Policy. The organization shall process personal information lawfully, fairly, transparently, and only for legitimate organizational purposes.

In managing personal data, ILA shall:

a. collect only information that is necessary for legitimate organizational functions;

b. process personal data in accordance with applicable laws and organizational policies;

c. maintain the confidentiality of whistleblowers, complainants, witnesses, respondents, and other affected persons;

d. implement appropriate technical and organizational safeguards against unauthorized access, disclosure, alteration, loss, or destruction of personal data;

e. ensure that personal data is accurate, relevant, and kept up to date where necessary;

f. limit access to personal data to authorized personnel with a legitimate need to know;

g. ensure secure transmission and storage of sensitive information;

h. report personal data breaches in accordance with applicable legal and donor requirements;

i. respect the privacy and dignity of all individuals involved in fraud prevention, reporting, and investigation processes; and

j. comply with the organization's Data Protection and Privacy Policy and any applicable national laws and donor data protection obligations.

All employees, Board members, volunteers, interns, consultants, contractors, and partners who have access to confidential information or personal data are responsible for maintaining its confidentiality and shall remain bound by these obligations even after the termination of their employment, engagement, or contractual relationship with ILA.

CHAPTER SIXTEEN

TRAINING, CAPACITY BUILDING AND AWARENESS

16.1 Staff Induction

The Initiative for Legal Aid (ILA) recognizes that an informed workforce is one of the most effective safeguards against fraud, corruption, and unethical conduct. Every individual associated with the organization shall understand their responsibilities under this Policy from the commencement of their engagement.

All newly recruited employees, Board members, volunteers, interns, consultants, contractors, and other representatives shall undergo mandatory induction training on the Anti-Fraud, Anti-Corruption and Whistleblowing Policy before assuming their duties or as soon as practicable thereafter.

The induction programme shall include, at a minimum:

a. ILA's commitment to integrity, accountability, transparency, and zero tolerance for fraud and corruption;

b. key provisions of this Policy;

c. ethical standards and expected conduct;

d. fraud and corruption risks within the organization;

e. conflict of interest obligations;

f. whistleblowing procedures and reporting channels;

g. confidentiality requirements;

h. protection against retaliation;

i. individual responsibilities for fraud prevention and detection;

j. disciplinary and legal consequences of policy violations; and

k. acknowledgement of understanding and commitment to comply with this Policy.

Completion of induction training shall be documented and maintained as part of personnel records.

16.2 Annual Refresher Training

ILA shall conduct periodic refresher training to reinforce awareness, strengthen organizational capacity, and ensure that all personnel remain informed of emerging fraud risks, changes in legislation, donor requirements, and organizational policies.

Refresher training shall ordinarily be conducted at least once every calendar year and may be delivered through workshops, seminars, webinars, e-learning platforms, or other appropriate methods.

Annual refresher training shall address, among other matters:

a. emerging fraud and corruption risks;

b. lessons learned from investigations and audits;

c. updates to organizational policies;

d. changes in applicable laws and regulations;

e. donor compliance requirements;

f. ethical decision-making;

g. cyber fraud and information security risks;

h. procurement integrity;

i. financial accountability; and

j. reporting obligations.

Attendance shall be monitored and documented to support organizational compliance and continuous learning.

16.3 Specialized Training

Certain positions within ILA involve heightened exposure to fraud risks and therefore require specialized technical training.

Specialized training shall be provided, as appropriate, to:

a. Board members;

b. senior management;

c. finance personnel;

d. procurement staff;

e. human resources personnel;

f. programme managers;

g. investigators;

h. internal auditors;

i. ICT personnel;

j. grants management staff; and

k. legal officers.

Specialized training may cover:

a. fraud risk assessment methodologies;

b. forensic investigation techniques;

c. financial fraud detection;

d. procurement fraud prevention;

e. digital evidence preservation;

f. cyber security and cyber fraud investigations;

g. interview techniques;

h. asset tracing and recovery;

i. donor compliance requirements;

j. regulatory reporting obligations; and

k. internal control strengthening.

ILA shall encourage relevant staff to participate in professional certification programmes and external capacity-building opportunities where resources permit.

16.4 Board Training

The Board of Directors has ultimate oversight responsibility for organizational integrity and governance. Accordingly, Board members shall receive periodic training to enable them to effectively discharge their oversight responsibilities under this Policy.

Board training shall include:

a. governance responsibilities relating to fraud prevention;

b. oversight of organizational risk management;

c. fiduciary duties;

d. conflict of interest management;

e. review of investigation reports;

f. whistleblower protection principles;

g. legal and regulatory obligations;

h. donor accountability requirements;

i. ethical leadership; and

j. oversight of internal control systems.

Board members shall remain informed of emerging governance risks affecting non-governmental organizations and best international practices in fraud prevention.

16.5 Partner Training

ILA recognizes that implementing partners, consultants, contractors, suppliers, and other third parties may expose the organization to fraud and corruption risks if they lack adequate awareness of organizational standards.

Where appropriate, ILA shall provide orientation or training to partners regarding:

a. anti-fraud obligations;

b. anti-corruption standards;

c. conflict of interest requirements;

d. procurement integrity;

e. reporting obligations;

f. whistleblowing mechanisms;

g. contractual compliance;

h. donor requirements;

i. safeguarding of organizational resources; and

j. consequences of policy violations.

Partnership agreements and contracts may require partners to participate in relevant compliance training as a condition of engagement.

16.6 Community Awareness

As an organization committed to promoting justice, accountability, and the rule of law, ILA shall undertake public awareness initiatives to encourage integrity, transparency, and responsible reporting of fraud and corruption within its programmes and operations.

Community awareness activities may include:

a. public education campaigns;

b. community dialogues;

c. stakeholder meetings;

d. radio programmes;

e. printed information materials;

f. social media engagement;

g. awareness workshops;

h. legal awareness sessions;

i. community complaint mechanisms; and

j. dissemination of information on available reporting channels.

These initiatives shall seek to enhance public confidence in ILA's commitment to accountability and encourage the reporting of suspected misconduct affecting the organization or its beneficiaries.

16.7 Donor Compliance Training

ILA acknowledges that development partners and donors often impose specific anti-fraud, anti-corruption, financial management, procurement, reporting, and compliance obligations as conditions of funding.

The organization shall ensure that relevant personnel receive training on applicable donor requirements before and during project implementation.

Donor compliance training may include:

a. donor anti-fraud and anti-corruption standards;

b. grant conditions and contractual obligations;

c. procurement requirements;

d. financial management standards;

e. reporting obligations;

f. documentation requirements;

g. eligibility of project expenditures;

h. fraud reporting procedures to donors;

i. audit preparedness;

j. monitoring and evaluation requirements;

k. sanctions for non-compliance; and

l. best practices for maintaining donor confidence and organizational credibility.

Project managers and other responsible personnel shall ensure that donor-funded activities are implemented in full compliance with applicable donor regulations, this Policy, and all related organizational policies.

ILA shall periodically evaluate the effectiveness of its training, capacity-building, and awareness programmes through participant feedback, assessments, audits, compliance reviews, and monitoring results. Lessons learned from these evaluations shall inform the continuous improvement of training materials and delivery methods to strengthen the organization's overall fraud prevention and integrity framework.

CHAPTER SEVENTEEN

MONITORING, COMPLIANCE, AUDIT AND REPORTING

17.1 Compliance Monitoring

The Initiative for Legal Aid (ILA) shall establish and maintain an effective monitoring system to ensure continuous compliance with this Anti-Fraud, Anti-Corruption and Whistleblowing Policy. Compliance monitoring is intended to identify weaknesses, assess the effectiveness of preventive measures, detect emerging fraud risks, and promote continuous organizational improvement.

The Executive Director shall ensure that appropriate mechanisms are in place to monitor compliance across all programmes, departments, projects, field offices, and donor-funded activities.

Compliance monitoring shall include, but not be limited to:

a. routine management supervision;

b. periodic compliance assessments;

c. review of financial and operational reports;

d. monitoring of procurement activities;

e. review of payroll administration;

f. monitoring implementation of corrective actions;

g. verification of policy compliance;

h. review of whistleblowing reports and trends;

i. monitoring implementation of audit recommendations; and

j. periodic fraud risk reviews.

Managers at all levels shall be responsible for monitoring compliance within their respective areas of responsibility and promptly reporting significant control weaknesses or suspected violations.

17.2 Internal Audit

The Internal Audit function shall provide independent and objective assurance on the adequacy, effectiveness, and efficiency of ILA's governance, risk management, internal control, and fraud prevention systems.

Internal Audit shall operate independently and shall have unrestricted access to all records, personnel, premises, systems, and information necessary to perform its duties, subject to applicable laws and confidentiality requirements.

Internal Audit responsibilities shall include:

a. evaluating the effectiveness of internal controls;

b. assessing compliance with this Policy and related organizational policies;

c. reviewing financial management systems;

d. examining procurement processes;

e. assessing asset management practices;

f. evaluating payroll controls;

g. identifying fraud vulnerabilities;

h. investigating suspected irregularities where authorized;

i. verifying implementation of corrective actions;

j. reporting significant findings to management and the Board; and

k. recommending improvements to strengthen organizational integrity.

Internal Audit reports shall be treated as confidential and shall be shared only with authorized persons.

17.3 External Audit

ILA shall engage independent external auditors in accordance with applicable laws, donor requirements, and organizational governance procedures.

External audits shall provide independent assurance regarding:

a. the fairness of financial statements;

b. compliance with donor agreements;

c. adequacy of financial controls;

d. compliance with applicable laws and regulations;

e. effectiveness of internal control systems;

f. safeguarding of organizational assets;

g. financial accountability; and

h. other matters required by applicable audit standards or donor agreements.

Management shall cooperate fully with external auditors by providing timely access to records, personnel, and relevant information.

Audit findings and recommendations shall be reviewed promptly, and corrective action plans shall be developed and implemented within reasonable timeframes.

17.4 Compliance Reviews

ILA shall periodically conduct formal compliance reviews to evaluate adherence to this Policy, related organizational policies, contractual obligations, donor requirements, and applicable legal standards.

Compliance reviews may be undertaken by Internal Audit, designated compliance personnel, external consultants, donor representatives, or other authorized reviewers.

Compliance reviews may assess:

a. implementation of fraud prevention measures;

b. effectiveness of whistleblowing mechanisms;

c. conflict of interest management;

d. procurement compliance;

e. financial management practices;

f. grant management;

g. records management;

h. investigation procedures;

i. disciplinary processes;

j. implementation of previous recommendations; and

k. overall organizational compliance culture.

The results of compliance reviews shall be documented, communicated to management, and used to strengthen organizational systems and controls.

17.5 Fraud Indicators

ILA shall establish mechanisms for identifying, monitoring, and responding to fraud indicators, commonly referred to as "red flags," that may signal the existence of fraud, corruption, or other irregularities.

Examples of fraud indicators include:

a. unexplained financial discrepancies;

b. unusual accounting adjustments;

c. missing supporting documentation;

d. repeated procurement irregularities;

e. unexplained lifestyle changes inconsistent with known income;

f. unauthorized access to organizational systems;

g. duplicate or suspicious payments;

h. fictitious vendors or employees;

i. frequent override of internal controls;

j. conflicts of interest that have not been disclosed;

k. unusual contract amendments;

l. manipulation of records;

m. repeated complaints regarding the same individual or process;

n. resistance to audits or investigations; and

o. other unusual transactions or behaviors that may indicate misconduct.

The existence of a fraud indicator shall not, by itself, constitute proof of wrongdoing but shall warrant appropriate review, inquiry, or investigation depending on the circumstances.

17.6 Annual Reports

Management shall prepare periodic reports on the implementation and effectiveness of this Policy, with a comprehensive annual report submitted to the Board of Directors.

The annual report may include:

a. the number of fraud and corruption allegations received;

b. whistleblowing reports submitted;

c. investigations conducted;

d. substantiated cases;

e. disciplinary actions taken;

f. financial losses identified and recovered;

g. corrective actions implemented;

h. fraud risk assessment results;

i. compliance monitoring activities;

j. audit findings relevant to fraud prevention;

k. staff training and awareness activities;

l. significant policy improvements; and

m. recommendations for strengthening organizational integrity.

Where required by law, contractual obligations, or donor agreements, relevant information shall also be reported to regulatory authorities and development partners in accordance with applicable reporting requirements, while maintaining appropriate confidentiality.

17.7 Key Performance Indicators

ILA shall establish measurable Key Performance Indicators (KPIs) to evaluate the effectiveness of its anti-fraud, anti-corruption, and whistleblowing framework and to promote continuous improvement.

Key Performance Indicators may include:

a. percentage of staff completing mandatory anti-fraud training;

b. percentage of Board members trained on governance and integrity;

c. number of fraud awareness activities conducted;

d. number of whistleblower reports received and acknowledged within prescribed timelines;

e. average time taken to assess and investigate reported cases;

f. percentage of substantiated cases resulting in appropriate corrective or disciplinary action;

g. implementation rate of audit and investigation recommendations;

h. percentage of high-risk fraud risks with mitigation measures implemented;

i. value of financial losses recovered following fraud investigations;

j. number of internal control improvements implemented;

k. percentage of procurement activities compliant with organizational policies;

l. percentage of donor-funded projects meeting anti-fraud compliance requirements;

m. reduction in repeat fraud incidents and control failures over time; and

n. overall compliance rating based on periodic internal audits and compliance reviews.

Management shall review these indicators at least annually and use the results to strengthen governance, allocate resources, enhance internal controls, and improve the effectiveness of fraud prevention and integrity initiatives.

CHAPTER EIGHTEEN

ROLES, RESPONSIBILITIES AND ACCOUNTABILITY

18.1 Board

The Board of Directors bears the ultimate responsibility for establishing and maintaining an effective Anti-Fraud, Anti-Corruption and Whistleblowing framework within the Initiative for Legal Aid (ILA). The Board shall demonstrate zero tolerance towards fraud, corruption and other forms of financial or ethical misconduct.

The Board shall:

a. approve this Policy and any subsequent amendments;

b. establish an ethical governance framework that promotes integrity, accountability and transparency;

c. provide strategic oversight of fraud risk management;

d. ensure adequate resources are allocated for fraud prevention, investigations and compliance;

e. review significant fraud cases and corrective actions;

f. oversee implementation of recommendations arising from investigations and audits;

g. ensure management maintains effective internal controls;

h. safeguard organizational assets and donor resources;

i. receive periodic reports on fraud risks, investigations and whistleblowing activities; and

j. promote a culture of accountability throughout the organization.

18.2 Executive Director

The Executive Director shall be responsible for the overall implementation of this Policy and shall ensure that fraud prevention forms an integral part of organizational management.

The Executive Director shall:

a. provide leadership in promoting ethical conduct;

b. ensure implementation of fraud prevention systems;

c. allocate adequate financial, human and technological resources;

d. ensure allegations of fraud are investigated promptly and fairly;

e. report significant fraud incidents to the Board and donors where required;

f. approve corrective and disciplinary measures;

g. ensure appropriate cooperation with law enforcement agencies;

h. monitor implementation of investigation recommendations; and

i. promote continuous improvement of fraud management systems.

18.3 Senior Management

Senior Management shall support implementation of this Policy across all departments and programmes.

Senior Management shall:

a. identify fraud risks within their respective departments;

b. implement effective preventive controls;

c. ensure staff comply with organizational policies;

d. encourage ethical conduct and transparency;

e. monitor departmental compliance;

f. immediately report suspected fraud;

g. support investigations;

h. implement corrective actions; and

i. ensure continuous staff awareness.

18.4 Finance

The Finance Department shall play a central role in preventing financial fraud and safeguarding organizational resources.

Finance personnel shall:

a. maintain accurate accounting records;

b. implement financial controls and segregation of duties;

c. verify supporting documentation before processing payments;

d. reconcile bank accounts and financial records regularly;

e. detect unusual financial transactions;

f. report suspicious financial activities immediately;

g. safeguard cash and financial assets;

h. cooperate during investigations;

i. support recovery of financial losses; and

j. comply with donor financial management requirements.

18.5 Procurement

The Procurement Unit shall ensure that all procurement activities are conducted fairly, competitively and transparently.

Procurement personnel shall:

a. comply with procurement policies;

b. avoid conflicts of interest;

c. ensure competitive bidding processes;

d. maintain complete procurement documentation;

e. verify supplier legitimacy;

f. monitor supplier performance;

g. report procurement irregularities;

h. prevent bid rigging and collusion;

i. ensure contract compliance; and

j. safeguard procurement integrity.

18.6 Human Resources

The Human Resources Department shall support fraud prevention through ethical recruitment, employee management and disciplinary processes.

Human Resources shall:

a. conduct employee background verification where appropriate;

b. ensure staff sign the Code of Conduct and this Policy;

c. maintain personnel records;

d. administer disciplinary procedures fairly;

e. coordinate fraud awareness training;

f. support whistleblower protection;

g. monitor staff compliance with disclosure requirements;

h. investigate employment-related misconduct jointly with management where necessary; and

i. maintain confidentiality throughout disciplinary processes.

18.7 ICT

The ICT Unit shall protect organizational information systems from cyber fraud and unauthorized access.

ICT personnel shall:

a. implement appropriate cybersecurity controls;

b. maintain secure access controls;

c. monitor network activities;

d. maintain audit logs;

e. investigate suspected cyber incidents;

f. safeguard electronic evidence;

g. ensure secure data backup and disaster recovery;

h. protect confidential organizational information;

i. support digital forensic investigations where required; and

j. ensure compliance with ICT security policies.

18.8 MEAL

The Monitoring, Evaluation, Accountability and Learning (MEAL) Unit shall support fraud prevention through programme monitoring and accountability mechanisms.

The MEAL Unit shall:

a. monitor programme implementation for fraud indicators;

b. verify reported project results;

c. ensure beneficiary accountability mechanisms are functional;

d. document complaints received through accountability systems;

e. identify programme irregularities;

f. share findings with management for corrective action;

g. support risk assessments;

h. monitor implementation of corrective actions; and

i. strengthen organizational learning from fraud incidents.

18.9 Programme Staff

All programme staff shall conduct project activities honestly and in accordance with organizational policies.

Programme staff shall:

a. protect programme resources;

b. report suspected fraud immediately;

c. maintain accurate programme records;

d. avoid conflicts of interest;

e. comply with donor requirements;

f. verify beneficiary information where applicable;

g. cooperate with investigations;

h. protect confidential information; and

i. uphold organizational values at all times.

18.10 Volunteers

Volunteers engaged by ILA shall adhere to the same ethical standards expected of employees.

Volunteers shall:

a. comply with this Policy;

b. report suspected fraud or corruption;

c. maintain confidentiality;

d. avoid misuse of organizational resources;

e. declare conflicts of interest;

f. cooperate with investigations; and

g. uphold the reputation of ILA.

18.11 Consultants

Consultants providing services to ILA shall comply with all applicable organizational policies, contractual obligations and professional ethical standards.

Consultants shall:

a. avoid fraudulent, corrupt or unethical conduct;

b. disclose conflicts of interest;

c. protect confidential information;

d. maintain accurate records of work performed;

e. report suspected misconduct;

f. cooperate fully during investigations;

g. comply with contractual anti-fraud clauses; and

h. remain accountable for any fraudulent acts committed during the course of their engagement.

18.12 Partners

Implementing partners, consortium members and collaborating organizations shall maintain fraud prevention systems consistent with this Policy.

Partners shall:

a. establish effective internal controls;

b. comply with donor and contractual obligations;

c. maintain transparent financial records;

d. report fraud affecting jointly implemented programmes;

e. permit audits and investigations;

f. cooperate in recovery of losses;

g. protect whistleblowers; and

h. implement agreed corrective actions.

18.13 Suppliers

All suppliers, contractors, vendors and service providers engaged by ILA shall conduct business with honesty, fairness and integrity.

Suppliers shall:

a. comply with applicable laws and contractual obligations;

b. refrain from bribery, fraud, collusion and corruption;

c. avoid offering gifts intended to improperly influence decisions;

d. disclose conflicts of interest;

e. maintain accurate invoices and supporting documentation;

f. cooperate with audits and investigations;

g. permit verification of contract performance where required;

h. immediately report suspected fraud affecting ILA contracts; and

i. acknowledge that violations of this Policy may result in contract termination, recovery of losses, debarment from future engagements, and referral to competent authorities where appropriate.

CHAPTER NINETEEN

POLICY IMPLEMENTATION

19.1 Implementation Strategy

The Initiative for Legal Aid (ILA) shall implement this Anti-Fraud, Anti-Corruption and Whistleblowing Policy through a structured, organization-wide approach that integrates fraud prevention, detection, reporting, investigation and accountability into all organizational operations. Implementation shall be guided by the principles of good governance, transparency, accountability, participation, continuous improvement and compliance with applicable laws, donor requirements and international best practices.

The implementation strategy shall seek to:

a. integrate fraud risk management into organizational planning and decision-making;

b. strengthen internal controls across all departments and programmes;

c. promote ethical leadership and organizational integrity;

d. build staff capacity through continuous training and awareness;

e. strengthen reporting and whistleblowing mechanisms;

f. enhance monitoring, evaluation and compliance systems;

g. improve institutional resilience against fraud and corruption; and

h. foster continuous learning from investigations, audits and compliance reviews.

Implementation shall be phased where necessary and supported by annual operational plans and departmental work plans.

19.2 Action Plans

Management shall develop and maintain implementation action plans to operationalize this Policy.

The action plans shall:

a. identify specific implementation activities;

b. assign responsible departments and officers;

c. establish implementation timelines;

d. allocate required resources;

e. define measurable performance indicators;

f. identify implementation risks and mitigation measures;

g. establish monitoring mechanisms; and

h. provide periodic progress updates to Senior Management and the Board.

Departmental action plans shall be reviewed periodically to ensure continued relevance and effectiveness.

19.3 Institutional Responsibilities

Implementation of this Policy shall be a shared responsibility across the organization.

Responsibilities shall include:

Board of Directors

a. provide strategic oversight;

b. approve major policy revisions;

c. monitor organizational compliance.

Executive Director

a. provide leadership for implementation;

b. allocate resources;

c. ensure institutional accountability.

Senior Management

a. supervise departmental implementation;

b. monitor compliance;

c. address identified weaknesses.

Department Heads

a. implement policy requirements within their departments;

b. maintain effective internal controls;

c. monitor staff compliance.

All Employees, Volunteers, Consultants and Partners

a. comply with this Policy;

b. report suspected misconduct;

c. participate in training programmes;

d. cooperate with investigations and audits.

Implementation responsibilities shall be reflected in job descriptions, performance evaluations and contractual obligations where appropriate.

19.4 Resource Allocation

ILA shall allocate adequate financial, human, technical and administrative resources necessary for effective implementation of this Policy.

Resources may include:

a. staff responsible for compliance and investigations;

b. fraud awareness and ethics training programmes;

c. whistleblowing and reporting systems;

d. investigation resources;

e. secure information management systems;

f. audit and compliance activities;

g. digital security systems;

h. legal support services; and

i. monitoring and evaluation activities.

Where donor-funded projects require additional fraud prevention measures, management shall ensure sufficient resources are incorporated into project budgets whenever practicable.

19.5 Compliance Framework

ILA shall establish a comprehensive compliance framework to ensure consistent application of this Policy throughout the organization.

The compliance framework shall include:

a. regular compliance monitoring;

b. internal control assessments;

c. fraud risk assessments;

d. periodic internal audits;

e. external audits where applicable;

f. compliance reviews;

g. investigation follow-up;

h. management reporting;

i. corrective action monitoring; and

j. continuous policy improvement.

Failure to comply with this Policy may result in disciplinary, contractual, civil or criminal action, depending on the nature and seriousness of the violation.

19.6 Reporting

Management shall establish appropriate reporting mechanisms to monitor implementation of this Policy.

Reports may include:

a. fraud risk reports;

b. whistleblowing statistics;

c. investigation reports;

d. compliance reports;

e. internal audit findings;

f. implementation progress reports;

g. corrective action reports;

h. lessons learned from fraud incidents;

i. donor compliance reports where required; and

j. annual fraud management reports to the Board.

Reports shall be prepared periodically and used to strengthen organizational governance, accountability and continuous improvement.

CHAPTER TWENTY

POLICY REVIEW, AMENDMENT AND APPROVAL

20.1 Policy Review

This Policy shall be reviewed periodically to ensure that it remains current, effective and consistent with applicable laws, regulatory requirements, donor expectations and international best practices.

A comprehensive review shall ordinarily be conducted every three (3) years or earlier where necessary due to:

a. legislative or regulatory changes;

b. significant organizational restructuring;

c. emerging fraud risks;

d. changes in donor requirements;

e. recommendations arising from audits or investigations;

f. significant operational changes; or

g. decisions of the Board of Directors.

The review process shall assess the effectiveness of implementation, identify gaps and recommend necessary improvements.

20.2 Amendment Procedure

Amendments to this Policy may be initiated by the Board of Directors, the Executive Director or Senior Management where justified by operational needs or legal and regulatory developments.

The amendment process shall include:

a. identification of the proposed amendments;

b. consultation with relevant departments and stakeholders where appropriate;

c. legal and compliance review;

d. assessment of operational implications;

e. preparation of revised policy provisions;

f. approval by the competent authority; and

g. communication of approved amendments to all affected persons.

All amendments shall be documented and incorporated into the official version of the Policy.

20.3 Version Control

ILA shall maintain an effective version control system to ensure that only the current approved version of this Policy is in use.

Version control shall include:

a. policy version numbers;

b. approval dates;

c. effective dates;

d. review dates;

e. amendment history;

f. responsible policy owner;

g. document classification; and

h. controlled distribution records.

Superseded versions shall be archived securely for institutional reference and audit purposes.

20.4 Approval

This Policy shall become effective upon approval by the Board of Directors of the Initiative for Legal Aid (ILA).

The Board shall:

a. approve the initial Policy;

b. approve all substantive amendments;

c. monitor implementation through periodic reports; and

d. ensure organizational commitment to the principles contained in this Policy.

The Executive Director shall be responsible for communicating the approved Policy throughout the organization and ensuring its implementation.

20.5 Transitional Arrangements

Upon approval of this Policy:

a. all existing fraud prevention procedures shall, where necessary, be aligned with this Policy;

b. existing guidelines inconsistent with this Policy shall be revised or withdrawn;

c. staff, volunteers, consultants and partners shall receive appropriate orientation on the Policy;

d. implementation plans shall be developed within a reasonable period;

e. ongoing investigations shall continue under applicable procedures while incorporating the principles of this Policy where practicable; and

f. management shall monitor the transition process to ensure minimal disruption to organizational operations.

20.6 Effective Date

This Policy shall take effect on the date approved by the Board of Directors unless another effective date is specified in the Board Resolution.

The Policy shall remain in force until amended, replaced or repealed by the Board of Directors.

All employees, Board members, volunteers, interns, consultants, contractors, suppliers, implementing partners and other persons acting on behalf of ILA shall comply with this Policy from its effective date.