

SOCDA | ORGANIZATIONAL POLICY & PROCEDURES



SOMALI COMMUNITY DEVELOPMENT ASSOCIATION (SOCDA)

Empower • Engage • Develop

ANTI-FRAUD, ANTI-CORRUPTION & WHISTLEBLOWING POLICY

Prevention, detection, reporting and response to misconduct

SOCDA-AFC-POL-001

1. PURPOSE

The purpose of this Policy is to establish SOCDA's framework for preventing, detecting, reporting, investigating and responding to:

- Fraud
- Corruption
- Bribery
- Theft
- Embezzlement
- Financial misconduct
- Procurement fraud
- Conflict-of-interest abuse
- Misuse of organisational assets
- False claims
- Collusion
- Kickbacks
- Other forms of dishonest or unethical conduct

SOCDA has **zero tolerance for fraud and corruption.**

The organisation is committed to protecting:

- Donor funds
- Community resources
- Organizational assets
- Staff
- Beneficiaries
- Partners
- Its reputation and credibility

2. POLICY STATEMENT

SOCDA shall maintain a control environment designed to:

Prevent → Detect → Report → Investigate → Correct → Learn

All personnel have a responsibility to protect SOCDA's resources and report credible concerns.

No person shall be permitted to use their position within SOCDA for personal financial or other improper benefit.

3. SCOPE

This Policy applies to:

- Board members
 - Executive Director
 - Employees
 - Project staff
 - Consultants
 - Volunteers
 - Interns
 - Contractors
 - Suppliers
 - Partners where contractually applicable
 - Anyone acting on behalf of SOCDA
-

4. DEFINITIONS

4.1 Fraud

An intentional act of deception designed to obtain an improper benefit or cause a loss.

Examples:

- False invoices
- Fictitious employees
- Inflated expenses
- Falsified documents
- Misappropriation

4.2 Corruption

Abuse of entrusted authority for private gain.

4.3 Bribery

Offering, giving, receiving or requesting an improper benefit to influence a decision.

4.4 Embezzlement

Misappropriation of money or assets entrusted to an individual.

4.5 Kickback

An improper payment or benefit provided in return for favourable treatment.

4.6 Collusion

An agreement between two or more parties to improperly influence a decision.

4.7 Whistleblower

A person who raises a concern about suspected wrongdoing in good faith.

5. PROHIBITED CONDUCT

SOCDA prohibits:

- Fraud
- Bribery
- Corruption
- Theft
- Embezzlement
- Kickbacks
- Falsification
- Procurement manipulation
- Ghost employees
- False beneficiaries
- False reporting
- Unauthorised financial commitments
- Misuse of assets
- Concealment of financial irregularities
- Retaliation against whistleblowers

6. EXAMPLES OF FRAUD

Fraud may include:

Financial

- False expense claims.
- Duplicate payments.
- Manipulated receipts.
- Misappropriation of cash.
- Fictitious suppliers.
- Payroll fraud.

Procurement

- Bid manipulation.
- Supplier collusion.
- Favouritism.
- False quotations.
- Split purchases to avoid thresholds.
- Kickbacks.

Programme

- Inflated beneficiary numbers.
- Fictitious activities.
- False attendance lists.
- Misrepresentation of results.
- Diversion of programme resources.

HR

- Ghost employees.
- Falsified qualifications.
- Manipulation of recruitment.
- Unauthorized salary changes.

7. CORRUPTION RISKS

SOCDA recognises corruption risks may arise in:

- Procurement
- Recruitment
- Beneficiary selection
- Grant management
- Financial transactions
- Licensing
- Government engagement
- Partnerships
- Asset management
- Logistics
- Programme implementation

Risk assessments shall identify and address relevant risks.

8. BRIBERY

No SOCDA personnel may:

- Offer a bribe.
- Request a bribe.
- Accept a bribe.
- Facilitate bribery.

Personnel who are asked for a bribe should report the incident as soon as safely possible.

9. FACILITATION PAYMENTS

SOCDA does not authorize unofficial payments intended to accelerate routine government or administrative services.

Where staff face a serious security threat or coercion, safety takes priority.

Such incidents must be documented and reported as soon as reasonably possible.

10. KICKBACKS

A kickback is prohibited regardless of whether it is:

- Cash
- Gift
- Commission
- Employment opportunity
- Personal service
- Other benefit

Supplier and contractor agreements should include appropriate anti-corruption clauses.

11. PROCUREMENT FRAUD

Procurement personnel shall not:

- Manipulate quotations.
- Share confidential bids.
- Favour particular suppliers.
- Create false competition.
- Split purchases to bypass approval thresholds.
- Accept commissions.
- Alter evaluation results.

All significant procurement decisions must be documented.

12. FINANCIAL CONTROLS

SOCDA shall maintain controls including:

- Segregation of duties.
- Budget controls.
- Approval limits.
- Bank reconciliation.
- Cash controls.
- Supporting documentation.
- Supplier verification.
- Payroll controls.
- Asset registers.
- Periodic financial reviews.

13. SEGREGATION OF DUTIES

Where practical, different individuals should:

1. Initiate a transaction.
2. Review it.
3. Approve it.
4. Process payment.
5. Record it.
6. Reconcile it.

One person should not control the complete transaction cycle.

14. PROCUREMENT CONTROLS

SOCDA procurement should include:

- Approved procurement thresholds.
- Competitive quotations where required.
- Bid documentation.
- Evaluation criteria.
- Conflict declarations.
- Approval documentation.
- Supplier due diligence.
- Purchase orders/contracts.
- Delivery verification.

15. CASH CONTROLS

Cash should be minimised.

Where cash is necessary:

- Limits shall be established.
- Cash must be secured.
- Cash counts conducted.
- Advances tracked.
- Receipts retained.
- Reconciliation completed.

16. BANKING CONTROLS

SOCDA shall maintain:

- Approved bank signatories.
- Appropriate dual authorization.
- Bank reconciliations.
- Secure banking credentials.
- Regular review of signatory lists.

17. PAYROLL CONTROLS

SOCDA shall maintain controls over:

- Employee master data.
- Salary changes.
- Attendance/contract status where applicable.
- Payroll preparation.
- Payroll approval.
- Bank payment.
- Payroll reconciliation.

Ghost employees are strictly prohibited.

18. ASSET PROTECTION

SOCDA shall maintain an asset register.

Assets shall be:

- Identified.
- Assigned.
- Protected.
- Periodically verified.
- Properly transferred.
- Disposed of through authorized procedures.

19. PROGRAMME FRAUD

Programme teams shall ensure accurate:

- Beneficiary records
- Attendance records
- Activity reports
- Distribution records

- Monitoring data
- Results reporting

Fabricating Programme results is prohibited.

20. BENEFICIARY FRAUD AND DIVERSION

SOCDA personnel shall not:

- Divert assistance.
- Manipulate beneficiary lists.
- Demand money from beneficiaries.
- Demand sexual favors.
- Favor relatives or associates.
- Sell Programme assistance.

21. DONOR REPORTING INTEGRITY

All donor reports must be:

- Accurate.
- Evidence-based.
- Complete.
- Timely.
- Properly reviewed.

Personnel must not knowingly submit false:

- Financial reports
- Programme results
- Beneficiary figures
- Procurement information
- Expenditure reports

22. FRAUD RISK ASSESSMENT

SOCDA shall periodically assess fraud risks.

The risk assessment should consider:

Area	Risk
Finance	
Procurement	
Payroll	
Cash	
Programme	
Beneficiary selection	
Assets	
Partnerships	
Grants	
Recruitment	
Data	

Each identified risk should have:

- Risk rating
- Control
- Responsible person
- Mitigation action
- Review date

23. FRAUD REPORTING

Anyone may report suspected fraud.

Reports may be made through:

1. Immediate supervisor.
2. Finance Manager.
3. HR.
4. Executive Director.
5. Internal/Compliance focal point.
6. Board-designated channel.
7. Safeguarding/PSEA mechanism where relevant.

Serious concerns should bypass individuals implicated in the allegation.

24. CONFIDENTIAL REPORTING

Where practical, SOCDA shall provide confidential reporting channels.

Reports should be handled on a need-to-know basis.

Information should not be unnecessarily shared with:

- Colleagues
- Suppliers
- Partners
- Unauthorized managers

25. ANONYMOUS REPORTING

SOCDA may accept anonymous reports where feasible.

Anonymous reports should contain sufficient information to enable assessment.

Anonymous reporting should not be used to intentionally make malicious allegations.

26. WHISTLEBLOWER PROTECTION

SOCDA prohibits retaliation against anyone who reports concerns in good faith.

Retaliation includes:

- Threats
- Dismissal
- Demotion
- Harassment
- Intimidation
- Unfair treatment
- Punitive reassignment

Retaliation may constitute misconduct.

27. GOOD-FAITH REPORTING

A person does not need to prove fraud before reporting.

A report may be made where the person has reasonable grounds to suspect wrongdoing.

The investigation process determines whether the allegation is substantiated.

28. FALSE OR MALICIOUS REPORTS

Knowingly submitting false or malicious allegations may constitute misconduct.

However, an allegation that cannot be substantiated shall **not automatically be considered false**.

This distinction is essential to protect legitimate whistleblowing.

29. INITIAL ASSESSMENT

When a concern is received, the designated authority shall conduct an initial assessment to determine:

- Nature of allegation
- Credibility
- Potential financial loss
- Safeguarding implications
- Security implications
- Donor implications
- Legal implications
- Conflict-of-interest concerns

30. FRAUD RESPONSE CLASSIFICATION

Level	Description	Response
Low	Minor control concern	Management action
Moderate	Potential irregularity	Formal review

High	Credible fraud/corruption	Investigation + ED/Board notification
Critical	Major fraud, senior involvement or major donor/reputational risk	Immediate escalation + independent investigation

31. INVESTIGATION

Investigations should be:

- Independent where necessary.
- Objective.
- Confidential.
- Properly documented.
- Proportionate.
- Conducted without retaliation.

Investigators must disclose conflicts of interest.

32. INVESTIGATION PROCESS

The process should normally include:

Step 1

Receive allegation.

Step 2

Register allegation securely.

Step 3

Conduct preliminary assessment.

Step 4

Determine response level.

Step 5

Appoint investigator.

Step 6

Preserve relevant evidence.

Step 7

Conduct investigation.

Step 8

Document findings.

Step 9

Determine management action.

Step 10

Recover losses where appropriate.

Step 11

Notify donor/authorities where required.

Step 12

Strengthen controls and document lessons learned.

33. EVIDENCE PRESERVATION

Where fraud is suspected, SOCDA should protect relevant:

- Financial records
- Emails
- Procurement documents
- Contracts
- Receipts
- Electronic records

- Asset records
- Attendance records
- Programme documents

Records should not be altered or destroyed.

34. INVESTIGATION REPORT

A formal investigation report should normally contain:

1. Background.
2. Allegation.
3. Scope.
4. Methodology.
5. Evidence reviewed.
6. Findings.
7. Conclusions.
8. Financial impact.
9. Control weaknesses.
10. Recommendations.

35. FINANCIAL RECOVERY

Where SOCDA establishes financial loss, it may pursue recovery through:

- Voluntary repayment.
- Salary recovery where legally permitted.
- Contractual recovery.
- Insurance.
- Supplier recovery.
- Legal remedies.

Recovery decisions should consider applicable law and employment/contractual requirements.

36. DONOR NOTIFICATION

Where required by a grant agreement or donor policy, SOCDA shall notify the relevant donor of significant fraud or financial irregularity.

The Grants/Compliance function should maintain a donor notification matrix.

37. REPORTING TO AUTHORITIES

SOCDA may report matters to competent authorities where:

- Required by law.
- Required by donor agreement.
- Necessary to protect people or assets.
- Appropriate based on the nature of the offence.

Any such action should consider confidentiality, safety and legal requirements.

38. SAFEGUARDING INTERFACE

Where an allegation involves:

- Sexual exploitation
- Sexual abuse
- Child abuse
- Sexual harassment
- Other safeguarding concerns

the matter must also follow SOCDA's safeguarding procedures.

Safeguarding cases should not be treated solely as financial investigations.

39. BOARD OVERSIGHT

The Board shall receive appropriate information regarding:

- Significant fraud allegations.
- Major investigations.
- Confirmed financial losses.
- Serious control weaknesses.
- Major corrective actions.

Confidential personal information should only be shared where necessary.

40. MANAGEMENT RESPONSIBILITIES

The Executive Director shall ensure that:

- Controls are implemented.
- Staff understand the Policy.
- Allegations are appropriately handled.
- Serious cases are escalated.
- Corrective actions are followed.
- Lessons are incorporated into systems.

41. FINANCE RESPONSIBILITIES

Finance shall:

- Maintain financial controls.
- Identify unusual transactions.
- Conduct reconciliations.
- Support investigations.
- Preserve financial evidence.
- Report material irregularities.

42. INTERNAL CONTROL MONITORING

SOCDA should periodically review:

- Bank reconciliations
- Cash counts
- Advances
- Payroll
- Procurement
- Supplier records
- Assets
- Budget variances
- Supporting documents

43. RED FLAGS

Personnel should be alert to indicators such as:

Procurement

- Repeated awards to the same supplier.

- Identical quotations.
- Unusual urgency.
- Missing documentation.
- Supplier relationships with staff.

Finance

- Unusual transactions.
- Round-number payments.
- Repeated cash withdrawals.
- Missing receipts.
- Unexplained advances.

HR

- Duplicate bank accounts.
- Employees with limited documentation.
- Unusual salary changes.
- Unverified staff.

Programme

- Identical beneficiary signatures.
- Inflated attendance.
- Unusual distributions.
- Results inconsistent with field evidence.

44. FRAUD RISK REGISTER

SOCDA shall maintain a Fraud Risk Register.

Risk	Area	Likelihood	Impact	Rating	Existing Control	Mitigation	Owner
------	------	------------	--------	--------	------------------	------------	-------

45. FRAUD INCIDENT REGISTER

A restricted-access register should capture:

Incident No.	Date	Category	Location	Reported By	Status	Action
--------------	------	----------	----------	-------------	--------	--------

Access shall be strictly controlled.

46. ANTI-FRAUD TRAINING

All relevant staff should receive training on:

- Fraud awareness
- Red flags
- Procurement integrity
- Financial controls
- Whistleblowing
- Conflict of interest
- Safeguarding & Reporting mechanisms

47. SUPPLIER AND PARTNER REQUIREMENTS

SOCDA may require contracts to include provisions covering:

- Anti-bribery
- Fraud prevention
- Conflict of interest
- Audit/access rights
- Record retention
- Reporting obligations
- Termination for serious misconduct

48. RECORD RETENTION

Fraud-related records shall be retained securely for the period required by:

- Applicable law
- Donor requirements
- SOCDA's record retention policy

49. NON-COMPLIANCE

Failure to comply with this Policy may result in:

- Corrective action
- Disciplinary action

- Recovery of losses
- Contract termination
- Donor notification
- Referral to authorities

50. MONITORING INDICATORS

SOCDA should monitor:

Indicator	Target
Staff trained on anti-fraud policy	100%
Annual fraud-risk assessment completed	100%
Reported cases registered	100%
Significant allegations assessed	100%
Confirmed cases appropriately resolved	100%
High-risk audit findings followed up	≥90%
Staff aware of reporting mechanisms	≥90%
Annual Board fraud-risk review	100%

51. WHISTLEBLOWING REPORT FORM

Date: _____

How was the concern identified?

What happened?

Who is involved?

When did it happen?

Where did it happen?

Estimated financial impact, if known:

Evidence available:

Are you requesting confidentiality?

☐ Yes

☐ No

Name (optional): _____

Contact (optional): _____

52. FRAUD INVESTIGATION ACTION TRACKER

Action	Responsible	Deadline	Status	Evidence
Secure evidence				
Preliminary assessment				
Appoint investigator				
Investigation				
Management decision				
Recovery				
Donor notification				
Control improvement				

53. ANNUAL ANTI-FRAUD REPORT

Management should provide the Board with an annual summary covering:

- Fraud risk profile
- Number of reported concerns
- Categories of concerns
- Confirmed cases
- Financial impact
- Recovery
- Corrective actions
- Control improvements
- Training
- Outstanding cases

Reports should protect confidential information.

54. POLICY IMPLEMENTATION CHECKLIST

Before implementation:

- Board approval.
- Staff awareness.
- Whistleblowing channels established.
- Fraud Risk Register created.
- Fraud Incident Register created.
- Investigation procedure established.
- Board escalation mechanism established.
- Donor notification matrix created.
- Anti-fraud training conducted.
- Supplier clauses updated.
- Financial controls reviewed.
- Procurement controls reviewed.

55. APPROVAL

Approved by: SOCDA Governing Board

Board Resolution No.: _____

Chairperson: _____

Signature: _____

Date: _____

Effective Date: _____

Next Review Date: _____