European Union

DIGITAL EMPOWERMENT foundation

Fraud Prevention & Control Policy

Contents

OBJECTIVE

To address the risk of fraud and to lay out actions regarding identify responsibilities for preventing, detecting, reporting, and investigating processes, the programme will take when any suspected fraud is reported or discovered.

OVERVIEW

The programme "Soochna Seva" is committed to the highest standards of moral and ethical behavior towards the targeted population and with the employees too. The Breaches of these standards, especially through acts involving fraudulent, unethical and other dishonest behavior, are not only costly, but they tend to erode the trust of the community and confidence in the integrity of the stakeholders. By issuing this formal policy statement, the Programme hereby reaffirms its longstanding duty and responsibility to aggressively combat such behavior.

This policy is intended to

- Communicate a "zero tolerance" for fraudulent, unethical and other dishonest activities;
- Institute preventive measures designed to deter these activities or make them easier to detect and stop fraudulent activities;
- Provide for the reporting and investigation of such, including providing protection to persons who report violations; and
- Apply to any situation of fraud or suspected fraud involving programme employees, local partners, vendors, contractors, consultants, outside agencies, and/or any other parties having relationship with "Soochna Seva" or its personnel.

DEFINITION:

Fraud generally involves a willful or deliberate act or omission with the intention of obtaining an unauthorized benefit, service, property or something of value by deception, misrepresentation or other unethical or unlawful means. Fraud can be committed through many methods, including mail, wire, telephone and the Internet. Fraudulent, unethical and other dishonest acts may include, but are not limited to:

- Forgery or unauthorized alteration of documents or computer records;
- Falsification or misrepresentation of reports to management and external agencies, including time sheets, official travel claims for reimbursement or other expense reimbursement reports;
- Authorizing or receiving payment for time not worked;
- Misappropriation and Misutilization of funds, securities, supplies or other assets;
- Impropriety in handling or reporting of money or financial transactions;
- Engaging in activities that result in a conflict of interest;
- Disclosing confidential or proprietary information to unauthorized individuals;
- Removal of programme property, records or other assets from the premises without formal written/documented supervisory approval;
- Unauthorized use or destruction of programme property, records or other Project based assets;
- Taking information and using it or providing the information that would lead to identity theft;
- Use of programme property and resources for personal activities.

POLICY CONTENT AND GUIDELINES

Duty to Report

a. An individual who is aware of or suspects fraudulent activity must promptly report such activity to the Soochna Seva Programme Manager or the Human Resources Representative of DEF.
b. An individual who reports a suspicion of fraud regarding another individual or the organisation in good faith will in no circumstances be threatened, intimidated, or dismissed because he or she acted in accordance with this policy.
c. The programme manager will notify either the director, as appropriate, of the suspected fraud.
d. If the Human Resource representative determines that an investigation is warranted, an investigation team will be established with a written approval from CEO of Digital Empowerment Foundation.

In all cases, neither the employee nor the supervisor shall confront the accused individual(s), investigate the suspected activity, or discuss the matter with anyone other than the person or office to whom the activity was reported. Employees who knowingly make false allegations may be subject to disciplinary action up to and including dismissal. Allegations that are investigated and deemed unsubstantiated are not necessarily indicative of false allegations.

Responsibility for detection, reporting and prevention

Administrators and managers at all levels shall set the appropriate tone by displaying the proper attitude toward complying with laws, rules and regulations. Administrators and managers are also responsible for establishing and maintaining proper internal controls that will provide for the security and accountability of the resources entrusted to them. Such controls include, but are not limited to, ensuring that

a. incompatible duties are properly separated,
b. financial transactions are properly authorized and approved,
c. reports of financial activity are periodically reviewed for completeness and accuracy,
d. official personnel actions (ex: appointments, terminations, promotions) and employee time and leave is properly authorized and approved,
e. assets are physically secured,
f. computer passwords are protected and not shared,
g. confidential and sensitive information is protected from unauthorized access and
h. employees are effectively supervised

In addition, administrators shall be cognizant of the risks and exposures inherent in their area of responsibility, take appropriate steps to help mitigate those risks and be aware of the related symptoms of fraudulent, unethical and other dishonest actions.

Investigation

During the investigation, the Constitutional rights of all persons are to be observed. The accused will be afforded the opportunity to respond to the allegations or matters being investigated. The rights of the accused will be safeguarded throughout the investigation.

(a) The investigation team will be responsible for collecting all relevant information in respect of the fraud allegation.

(b) All employees are to cooperate fully with those performing an investigation pursuant to this policy. An employee who does not fully cooperate with an authorized investigation may be disciplined, up to and including termination of employment. An employee may be required to answer any questions that are within the scope of the employee's employment, whether such questions are asked in an investigation conducted by the DEF's Human Resources Department along with OPMU.

(c) Depending on the nature and seriousness of the alleged fraud, the Investigation Team may consult with, or engage the services of, other persons (such as technical experts with IT or forensic accounting skills) as well as external agencies (e.g. the Police and the Lawyer).

(d) The investigation team will have:

- free and unrestricted access to all Project records and premises, whether owned or rented; and
- the authority to examine, copy, and/or remove all, or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who may use or have custody or any such items or facilities, within the scope of the investigation.

(e) If the investigation team concludes that the evidence it has collected does not support the allegation of fraud, that outcome shall be reported confidentially to the individual who was suspected of fraud and to the complainant. A confidential report will be provided to the Human Resource Representative as appropriate that sets out the investigation process undertaken and the conclusions reached. The disclosure of that report or any part of that report to any other person will be determined by the CEO and OPMU only.

(f) In Case of Site offices/location other than New Delhi, OPMU will be responsible to take the necessary actions on any identified/reported fraud & shall appoint one Investigation officer from DPMU (District Project Management Unit) to investigate it further. Both units shall submit the Investigation reports within 30 days to Human Resource Department of DEF.

Actions

Where a suspected fraud is proved, the following procedures will takes place:

(a) Direct the DPMU of the project where the fraud has taken place, to put controls into place to mitigate further losses and prevent reoccurrence of similar misconduct.

(b) Review the reasons for the incident, the measures taken to prevent a recurrence, and any action needed to strengthen future responses to fraud;

(c) Keep all other relevant personnel suitably informed about the incident, including the Communications Manager on the Project.

(d) Employees determined to have participated in fraudulent, unethical or dishonest acts will be subject to disciplinary action in accordance with any applicable collective bargaining agreements, and DEF's personnel policies and rules.

(e) Such determination must be made with the consultation of the Department of Human Resources. Criminal, civil and/or other administrative actions may also be taken against employees who are found to have participated in unlawful acts.

(f) Everyone, regardless of classification, who fails to report fraudulent activity, as required by this policy, is subject to disciplinary action as decided by Digital Empowerment foundation's Human Resource Department and OPMU.

RECOVERY OF LOSS

Recovering losses of money or property is a major objective of the Project following any fraud investigation. The amount of any loss will be quantified as far as possible and repayment or reparation will normally be sought.

AUTHORIZED UNIT

Soochna Seva declares that OPMU (Overall Project Management Unit) and Human Resource Department of DEF will constitute the Authorization unit to ensure the appropriate execution of the 'Fraud prevention policy' in the organization.