ecsecc
eastern cape socio economic consultative council

FRAUD PREVENTION STRATEGY AND PLAN

Policy Category: Governance

Document Information

Revision History

Version	Primary Author	Summary of Changes	Date
1	Chief Financial Officer	Policy Update for Internal audit recommendation – Fraud Report dated January 2019	02 June 2019

Review

This document shall be reviewed every three years unless warranted sooner

Office responsible for review
Chief Financial Officer's Office

Approval

Name	Position	Signature	Date
Mr. Luvuyo Mosana	Acting Chief Executive Officer	LMosana	07 August 2019
Ms. Loren Smith	Chairperson of Audit Risk and ICT Board Sub-Committee		15 August 2019
Ms. Nomakhosazana Meth	Chairperson of the Board of Directors		29 August 2019

Contents

1 Scope

The purpose of this fraud prevention strategy and plan is to articulate ECSECC approach in reducing the risk of fraud from occurring, detecting it when it occurs and taking appropriate corrective action to remedy the harm caused by the breakdown in internal controls.

As required by sections 3.2.1 and 27.2.1 of the Treasury Regulations and in line with the organization's fraud prevention policy which states that risk assessment must be conducted on regular basis and a risk management strategy, which includes a fraud prevention plan, be used to direct internal audit effort; ECSECC has developed this fraud prevention strategy and plan.

This strategy and plan shall apply to all employees, stakeholders, contractors, vendors/suppliers and any other party doing business with the Entity. Further, this document must be read together with ECSECC's Fraud Prevention Policy and Code of Ethics.

2 Fraud risk management strategies

ECSECC's approach in reducing the risk of fraud comprises of three elements:

- Prevention Strategies;
- Detection Strategies; and
- Response Strategies.

3 Prevention strategies

Prevention strategies are designed to help reduce the risk of fraud and corruption from occurring in the first place. Leadership and governance structures are critical in ensuring oversight on programs to mitigate the risk of fraud and corruption. The Board together with senior management are responsible for setting the "tone at the top" and ensuring institutional support for ethical and responsible business practices at the highest levels of the entity. Principal oversight for fraud risk management has been delegated to the Audit, Risk and ICT Committee.

In being part of leading by example, senior management will ensure that all employees and stakeholders are made aware of the entity's fraud and corruption prevention strategies through various initiatives of awareness and training.

All employees are to be committed in eradicating fraud and corruption and ensuring that the entity strives to be perceived as ethical in all its dealings with the public and other interested

parties. In this regard, senior management, under the direction of the Board, will ensure that it does not become complacent in dealing with fraud and corruption.

In ensuring effective and efficient fraud prevention, the entity will employ the following:

3.1 Fraud risk assessment

Annually the entity will conduct an organization wide risk assessment. This will assist the entity in understanding the risks that are unique to the organization's operation which might lead to fraud, identify gaps and weaknesses in controls to mitigate those risks and develop a practical action plan for reducing such risks. While management is responsible for performing risk assessment and implementing action plans, the Audit, Risk and ICT Committee will review such assessment and action plans to ensure that these remain an ongoing effort and employ the assistance of the internal audit function in the assessment of the results.

3.2 Code of conduct

The entity is required to conduct itself in an ethical and moral way. The entity's code of conduct is the most important vehicle to be used in communicating key standards of acceptable business conduct. Annually, employees are required to acknowledge in writing understanding and adherence to the entity's code of conduct (the code of conduct is available from the Human Resource Division or shared drive).

3.3 Employee and third-party due diligence

The entity shall exercise due diligence in the recruitment of employees and dealing with suppliers.

5.3.1 Human Resource Practices

The entity shall ensure the proper implementation of its human resources systems, policies and procedures, which incorporate fraud and corruption prevention practices. These practices can be found in the entity's Human Resource Policy.

The approaches indicated below are key to the entity's efforts in reducing risk of fraud in HR.

- Recruitment of employees

  Recruitment will be conducted in accordance with the requisite recruitment procedure. It will be a transparent process and all appointments will be confirmed only after due recommendation. Any person, involved in any decision-making process, who may have a conflict of interest, must declare such a conflict in writing to the HR unit and withdraw from any further procedures.

- Pre-employment screening

  Pre-employment screening will be carried out for all appointments, and evidence of such screening which include verification of formal qualifications claimed, identification, criminal record, credit (where applicable), etc., will be maintained by the HR unit. The screening process will be in terms of the entity's HR policy. Reference checking is an essential part of the selection process and falls within pre-screening of potential employees.

- On-going disclosure

  All employees will be obliged to declare their private business interests and potential conflict of interest on an annual basis. These will be Investigated, where necessary, and filed for safekeeping by the HR unit. Additionally, employees are required to sign annual declaration to acknowledge that they have read ECSECC Strategies, Policies, Plans, Procedures, etc. and understand their responsibility and accountability in terms of these documents. Further, as part of on-going disclosure, a vetting process to check criminal and/or credit record and/or qualifications of employees will be performed where risk is identified.

- Employee induction program

  Employee induction is an opportunity to introduce employees to the policies, procedures, culture and ethics of the organization. All new employees, interns, seconded employees and temporary/contract workers will undergo an induction program as per the HR Policy.

- Staff exit procedures

  The exit procedure for employees leaving the entity requires the return of assets and an exit interview. Steps will be taken to ensure that specific follow-up time frames are set to encourage managers to apply the requirement related to the return of assets more promptly. Further, the employee will be requested to furnish reasons for leaving the Entity and to disclose any other information they view to be in the best interest of the Entity to be aware of.

5.3.2 Supply Chain Practices

The supply chain practices are highly regulated to ensure reduced risk of fraudulent activities. The entity will ensure adherence to the Supply Chain Practices as stipulated by the National Treasury. These have been taken into account in the entity's Supply Chain and Financial Policy.

5.3.3 Other

Acceptance and offering of business courtesies, including gifts, by all employees of the entity should occur only within the ethical standards prescribed by the entity. All gifts and donations should be disclosed in the Gifts Register kept at the Reception Area and in the Finance Manager's office. Employees are strongly discouraged from accepting gift not given in good faith as this act may be seen as a corrupt activity.

3.4 Communication and training

The main purpose of fraud and corruption awareness training is to assist in the prevention, detection and reporting of fraud and corruption by raising the level of awareness as to how fraud and corruption is manifested in the workplace. In this regard, all employees will receive training on the following:

- Fraud and Corruption Prevention Strategy;
- Ethical and Code of Conduct Policy;
- Whistle blowing;
- How to respond to fraud and corruption; and
- Manifestations of fraud and corruption in the workplace.

The Chief Financial Officer shall be responsible for facilitating employee awareness and will arrange and schedule awareness sessions annually based on the fraud risk assessment performed in each year and training every 3 years with policy review.

New employees will be made aware of the fraud prevention strategy through their induction course.

3.5 Financial Systems and Controls

Appropriate finance policies and procedures are necessary to ensure appropriate internal control over financial management and to limit fraud and corruption risks. The effectiveness of the existing financial policies and procedures will also be tested during the course of the internal audits as part of risk management and shortcomings addressed.

The Chief Finance Officer will ensure that the financial systems and controls that are in place, address any perceived fraud and corruption risk areas. Proper segregation of duties should be taken into account in all policies and procedures.

Financial systems and controls also act as detection and response strategies to fraud prevention.

4 Detection strategies

Detective controls are designed to uncover fraud and corruption when it occurs. This may occur through:

1. Vigilance on the part of employees, including line management;
   Employees together with management should pay more attention to detail in performing their respective duties and report processes and procedures that are performed outside the entity's policies and procedures.
2. The internal audit function;
   This is an important function that can assist management in determining whether or not the entity's controls are working as intended. They can also facilitate an effective governance process through the evaluation of other characteristics including ethics and values, performance management, and the assessment and communication of risk.
   Since it is impossible to audit every fraud and corruption risk, management shall ensure the development of a comprehensive audit plan that is based upon risks identified through a formal risk assessment process.
3. Ad hoc management reviews;
   Unplanned reviews of records by either management or internal audit functions shall be employed as one of the measures of detecting possible fraud and corruption.

4. Anonymous reports

   The entity encourages anonymous reports of suspected instances of fraud and corruption. If an employee becomes aware of a suspected fraud, corruption or any irregularity or unethical behaviour, such issues should be reported in terms of this strategy and plan.

5. The application of detection techniques.

   The entity will ensure that strong internal controls are in place to ensure prevention and detection of fraud and corruption within the workplace. Where considered necessary; forensic data analysis will be employed in the detection of suspected fraud and corruption.

5 Response strategies

Response controls are designed to take corrective action and remedy the harm caused by the fraud and corruption.

In the event that fraud or corruption is detected or suspected, investigations will be initiated, and if warranted, disciplinary proceedings, prosecution and / or action aimed at the recovery of losses will be initiated.

1. Investigations

   Any reports of incidents of fraud and / or corruption will be confirmed by an independent investigation. Anonymous reports may warrant a preliminary investigation before any decision to implement an independent investigation is taken.

   Investigations will be undertaken by appropriately qualified and experienced persons who are independent of the division where investigations are required. This may be a senior manager within the Entity itself, an external consultant or a law enforcement agency. All investigations performed and evidence obtained will be in accordance with acceptable practices and legal requirements. Independence and objectivity of investigations are paramount.

   Any investigation initiated must be concluded by the issue of a report by the person/s appointed to conduct such investigations. Such reports will only be disseminated to those persons required to have access thereto in order to implement whatever action is deemed appropriate as a result of the investigation.

Investigations may involve one or more of the following activities:

a) Interviewing of relevant witnesses, internal and external, including obtaining statements where appropriate;
b) Reviewing and collating documentary evidence;
c) Forensic examination of computer systems;
d) Examination of telephone records;
e) Enquiries from banks and other financial Entity's (subject to the granting of appropriate approval/Court orders);
f) Enquiries with other third parties;
g) Data search and seizure;
h) Expert witness and specialist testimony;
i) Tracing funds / assets / goods;
j) Liaison with the police or other law enforcement or regulatory agencies;
k) Interviewing persons suspected of involvement in fraud and corruption; and
l) Report preparation.

Any investigation into improper conduct within the Entity will be subject to an appropriate level of supervision by Audit, Risk and ICT committee, having regard to the seriousness of the matter under investigation.

2. Disciplinary proceedings

The ultimate outcome of disciplinary proceedings may involve a person/s receiving written warnings or the termination of their services. All disciplinary proceedings will take place in accordance with the procedures as set out in the entity's disciplinary procedures.

3. Prosecution

Should investigations uncover evidence of fraud or corruption in respect of an allegation or series of allegations, the Entity will review the facts at hand to determine whether the matter is one that ought to be reported to the relevant law enforcement agency for investigation and possible prosecution.

Such reports must be submitted to the South African Police Service in accordance with the requirements of all applicable acts. The Entity will give its full cooperation to any such law enforcement agency including the provision of reports compiled in respect of investigations conducted.

4. Recovery action

Where there is clear evidence of fraud or corruption and there has been a financial loss to the Entity, recovery action, criminal, civil or administrative, will be instituted to recover any such losses.

In respect of civil recoveries, costs involved will be determined to ensure that the cost of recovery is financially beneficial to the entity.

5. Internal control review after discovery of fraud

In each instance where fraud is detected, Line Management will reassess the adequacy of the current internal control environment (particularly those controls directly impacting on the fraud incident) to consider the need for improvements.

The responsibility for ensuring that the internal control environment is reassessed and for ensuring that the recommendations arising out of this assessment are implemented will lie with Line Management of the division concerned.

A report will be tabled at the Audit, Risk and ICT Committee on the internal control review performed by management in strengthening systems after the committed fraudulent activity.

6 Procedures for reporting suspected fraud and corruption

If an employee has a concern about fraud and corruption, it is hoped he/she will feel able to raise it first with his/her supervisor, thereafter his/her Senior Manager. It could also be raised with the Chief Executive Officer. Thereafter the issue should be raised with the Audit, Risk and ICT Committee. This may be done verbally or in writing. It must be stated whether he/she wishes to raise the matter in confidence so that they can make appropriate arrangements.

If these channels have been followed and the employee still has a concern or feels that the matter is so serious that it cannot be discussed with any of the above, then the matter must be raised via the processes that are available to the public.

To ensure that allegations are considered consistently, the Chief Financial Officer will report to the Audit, Risk and ICT committee on a quarterly basis as to the status of reports.

The matter can be raised by a member of the public through the following channels: -

- The National Toll-Free Service for the public sector is available to the public without access to the internet 0800 701 701. A quarterly report is requested by the Chief Financial Officer and tabled at the Risk, Audit and ICT Committee.
- Directly with the entity's internal auditors. Link is available on www.ecsecc.org or on request from the Chief Financial Officer.
- Directly to the Chief Executive Officer via post:

  ECSECC

  The Chief Executive Officer

  Postnet Vincent

  Private Bag X9063

  Suite 302,

  Vincent, 5247

7 How the reported matter will be handled

Once a concern is raised, it will be assessed to decide what action should be taken. This may involve an internal inquiry or a more formal investigation.

The issue raised will be acknowledged within seven working days. If it is requested, an indication of how the matter will be dealt with and a likely time scale could be provided. If the decision is made not to investigate the matter, reasons will be given. The whistle blower will be informed of who will be handling this matter, how to contact him/her and whether further assistance may or will be needed.

When a concern is raised, the whistle blower may be asked how he/she thinks the matter might best be resolved. If the whistle blower has any personal interest in the matter, it should be made known from the outset. If the concern falls more properly within the Grievance Procedure, he/she will be informed accordingly. Whistle blowers will be given as much feedback as possible, but full information may not always be given on the precise action taken where this could infringe a duty or confidence owed to someone else.

8 What is whistle blowing

The term whistle-blowing is generally used to describe the process of disclosing information relating to malpractice or mistreatment which members of staff may have

come across during the course of their work and which they feel would put the interest of the public and the entity at risk.

9 Employee confidence

In view of the protection offered to an employee raising a bona fide concern, it is preferable that the individual puts his/her name to the disclosure. ECSECC will not tolerate the harassment or victimization of anyone raising a genuine concern.

However, an employee may nonetheless wish to raise a concern in confidence. If he/she wishes that his/her identify must not be divulged, it will not be disclosed without consent. However, management expects the same confidentiality regarding the matter from employees.

If the situation arises where the matter could not be resolved without revealing an employee's identity (for example where his/her evidence is needed in court), it will be discussed with him/her on how and whether it can be proceeded with.

10 Protection of whistle blowers

The entity will ensure that an employee who makes a disclosure in the abovementioned circumstances will not be penalized or suffer from occupational detriment for doing so. Occupational detriment as defined by the Protected Disclosures Act, Act 26 of 2000, includes being dismissed, suspended, demoted, transferred against his/her will, harassed or intimidated, refused a reference or being provided with an adverse reference, because of his/her disclosure.

If a concern is raised in good faith, an employee will not be at risk of losing his/her job or suffering any form of retribution as a result.

This assurance is not extended to employees who maliciously raise matters they know to be untrue. Employees who do not act in good faith, who make an allegation without having reasonable grounds believing it to be substantially true, or who makes it maliciously or, may be subject to disciplinary proceedings.

11 Effective Date

The fraud prevention strategy and plan shall be effective from date of signature and shall apply prospectively.

12 Review Date

The fraud prevention strategy and plan shall be reviewed every 3 (three) years unless warranted sooner together with the fraud prevention policy and code of ethics policy.

ecsecc
eastern cape socio economic consultative council

12 Gloucester Road, Vincent, East London, 5217
Postnet Vincent, Private Bag X9063, Suite 302, Vincent, 5247

+27 (0)43 701 3400
+27 (0)43 701 3415
info@ecsecc.org
www.ecsecc.org

CELEBRATING 20 YEARS ECSECC 1995 - 2015