

# MPUMALANGA PROVINCIAL GOVERNMENT



## DEPARTMENT OF PUBLIC WORKS, ROADS AND TRANSPORT

### FRAUD POLICY

---

Revision Date:.....	None
Issue:.....	1.0
Responsible Section:.....	Risk Management
Approval Date:.....	None

---



## TABLE OF CONTENTS

TITLE	PAGE
ABBREVIATION	2
DEFINITIONS	2
INTRODUCTION	3
OBJECTIVES	3
REGULATORY FRAMEWORK	4
SCOPE OF APPLICATION	4
POLICY STATEMENT	5
ROLES AND RESPONSIBILITIES	14
MONITORING AND EVALUATION	15
POLICY REVIEW	16
APPROVAL	16

## 1. Definitions

Throughout this document, unless otherwise stated, the words in the first column below have the meanings stated opposite them in the second column (and cognate expressions shall bear corresponding meanings):

CFO	:	Chief Financial Officer of the Department
Code	:	Code of Conduct for Public Servants as prescribed in Chapter 2 of the Public Service Regulations, Regulations 1 of 2001
Committee	:	Fraud and Anti-Corruption Committee
Department	:	Mpumalanga Department of Public Works, Roads and Transport
EPWP	:	Expanded Public Works Programme
Fraud	:	the unlawful and intentional making of a misrepresentation resulting in actual or potential prejudice to another;
Corruption	:	giving or offering; receiving or agreeing to receive; obtaining or attempting to obtain any benefit which is not legally due to or by a person who has been charged with a duty or power by virtue of any employment, to do any act or omit to do any act in relation to that power or duty
Theft	:	the unlawful and intentional misappropriation of another's property or property which is in his/her lawful possession, with the intention to deprive the owner of its rights permanently".
GG	:	Government Garage
HOD	:	Head of Department of the Department
Hotline	:	Fraud Hotline

MEC	:	Member of Executive Committee responsible for the Department
PFMA	:	Public Finance Management Act 1 of 1999
Plan	:	Fraud Prevention Plan
Policy	:	Fraud Policy and Response Plan
Protected Disclosures Act	:	Protected Disclosures Act 26 of 2000
SAPS	:	South African Police Service

## 2. Introduction

The Fraud Policy is intended to set down the stance of the Department to fraud, as well as to reinforce existing systems, policies, procedures, rules and regulations of the Department aimed at deterring, preventing, detecting, reacting to and reducing the impact of fraud, where such dishonest activities subsist.

## 3. Policy Objective

The policy aims to:

- 3.1. Set down the stance of the Department to fraud,
- 3.2. Reinforce existing systems, policies, procedures, rules and regulations of the Department aimed at deterring, preventing, detecting, reacting to and reducing the impact of fraud, where such dishonest activities subsist.
- 3.3. Confirm that the Department supports and fosters a culture of zero tolerance to fraud in all its activities.



#### 4. Regulatory Framework

The legal and policy framework for formulating and implementing this policy is the –

- 4.1. Protected Disclosures Act, 2000 (Act No. 26 of 2000);
- 4.2. Whistle-blowing Guide for Public Sector Managers provided by the Department of Public Service Administration;
- 4.3. Public Service Act, 1994 (Proclamation No. 103 of 1994) and Regulations made in terms thereof;
- 4.4. Public Finance Management Act, 1999 (Act No. 1 of 1999) and Treasury Regulations issued in terms thereof
- 4.5. The National Public Service Anti-Corruption Strategy adopted by cabinet in 2002;
- 4.6. Labour Relations Act, 1995 (Act No.66 of 1995); and
- 4.7. Prevention and Combating of Corrupt Activities Act, 2004 (Act No.12 of 2004).

#### 5. Scope of Application

This policy applies to:

- 5.1. All allegations, attempts and incidents of fraud impacting or having the potential to impact the Department.
- 5.2. All employees of the Department must comply with the spirit and content of the Policy.



## 6. Policy Statement

The policy of the Department is Zero Tolerance to fraud. In addition, all fraud will be investigated and followed up by the application of all remedies available within the full extent of the law as well as the application of appropriate prevention and detection controls. These prevention controls include the existing financial and other controls and checking mechanisms as prescribed in the systems, policies, procedures, rules and regulations of the Department.

The efficient application of Treasury Regulations issued in terms of the PFMA, instructions contained in the policies and procedures of the Department, circulars and manuals of the Department, as well as other prescripts of the Public Service, in general, is one of the most important duties to be applied by every employee in the execution of their daily tasks and under no circumstances may there be a relaxation of the prescribed controls.

### 6.1. REPORTING PROCEDURES AND RESOLUTION OF REPORTED INCIDENTS

#### 6.1.1. What should an employee do if they suspect fraud?

- 6.1.1.1. Ideally, it is the responsibility of all employees to immediately report all allegations or incidents of fraud to their immediate manager or, if the employee has reason to believe that his/her immediate manager is involved, to the next level of management.

- 6.1.1.2. All managers are responsible for the detection, prevention and investigation of fraud and must report all incidents and allegations of fraud to the Senior Manager: Risk Management.
- 6.1.1.3. The Senior Manager: Risk Management will update the Committee and initiate an investigation into the matter, and consult with Senior Management with regard to steps to follow to resolve the matter. Where appropriate, the matter will be discussed with the Senior Manager: Labour Relations.
- 6.1.1.4. Should employees wish to report allegations of fraud anonymously, they can contact any member of management, the Senior Manager: Risk Management or alternatively report it directly to the National hotline number. The hotline, receives the information, screens it and supplies it to the Department.

#### **6.1.2. What should a member of the public do if they suspect fraud?**

- 6.1.2.1. The Department encourages members of the public who suspect fraud to contact the hotline.

#### **6.1.3. How will the Department deal with allegations of fraud?**

- 6.1.3.1. For issues raised by employees or members of the public, the action taken by the Department will depend on the nature of the concern. The matters raised may be investigated internally or referred to the South African Police Service.
- 6.1.3.2. Any fraud committed by an employee of the Department will not be tolerated and will be pursued by thorough investigation and to the full extent of the law, including consideration of:



- 6.1.3.2.1. Taking disciplinary action within a reasonable period of time after the incident;
  - 6.1.3.2.2. Instituting civil action to recover losses;
  - 6.1.3.2.3. Initiating criminal prosecution by reporting the matter to SAPS or any other relevant law enforcement agency; and
  - 6.1.3.2.4. Any other appropriate and legal remedy available.
- 6.1.3.3. In the event of departmental property being lost or stolen the responsible line/divisional manager or his/her authorised representative should ensure that the following steps are taken to report the incident:

## **6.2. Report to SAPS**

- 6.2.1. The theft/loss must be reported within 24 hours to SAPS, in the judicial area where the theft/loss occurred.

### **6.2.2. Statement/Affidavit to SAPS comprising**

The following must appear on the statement / affidavit to SAPS comprising:

- 6.2.2.1. A report in the form of a Sworn Affidavit or Affirmed Statement, made by the official discovering the theft/loss;
- 6.2.2.2. Full names and identity number of the deponent;
- 6.2.2.3. Full residential and business address, including telephone numbers of the deponent;
- 6.2.2.4. The day, date and time when the incident took place or was discovered;
- 6.2.2.5. Full particulars of the circumstances surrounding the theft/loss and the place where it occurred;
- 6.2.2.6. A full detailed description of the property stolen/lost, i.e. the type, brand name, model, serial number and any

Page 7



distinguishing features of the property, (which may identify it as Department property when found) must be given to SAPS for identification and circulation purposes;

- 6.2.2.7. A full description(s) of the suspect(s) must be given to SAPS;
- 6.2.2.8. Details (full names and addresses) of any witnesses, who could possibly supply any information of the incident/suspect, etc. who may have been present at the time of the incident must be given to SAPS; and
- 6.2.2.9. An official SAPS "case register" number and an (IB) Information Book number used for normal reports, must be obtained from SAPS.

### **6.3. Fraudulent or corrupt acts**

#### **6.3.1. Systems issues:**

Where a process/system exists which is prone to abuse by either employees or the public, e.g.:

- 6.3.1.1. Maladministration or financial misconduct in handling or reporting of money, financial transactions or other assets
- 6.3.1.2. Irregular collusion in the awarding of contracts, or orders for services and/or goods;
- 6.3.1.3. Disclosing confidential or proprietary information to outside parties;
- 6.3.1.4. Travel and subsistence claims (false charges for accommodation and meals; inflated charges on meals, false mileage claims); and
- 6.3.1.5. Abuse of sick or other permissible leave.

### **6.3.2. Financial issues:**

Where individuals or companies have fraudulently obtained money from the Department, e.g.:

- 6.3.2.1. Suppliers submitting invalid invoices or invoicing for work not done; and
- 6.3.2.2. Theft of revenue collected from tenants.

### **6.3.3. Equipment and resource issues**

Where Department's equipment and/or resources are used for personal use,

- 6.3.3.1. Misuse of Department's telephones for personal use;
- 6.3.3.2. Abuse of the Department's vehicles;
- 6.3.3.3. Theft of computers, inventory and cleaning materials; and
- 6.3.3.4. Irregular destruction, removal, or abuse of records (including intellectual property) and equipment;

### **6.3.4. Other issues:**

Activities undertaken by officers of Department which may be unlawful against Department's regulations or policies, fall below established standards or practices, or amount to improper conduct, e.g.:

- 6.3.4.1. Receiving undue gifts or favours for rendering services, e.g. expensive gifts in contradiction of the Code;
- 6.3.4.2. Nepotism and favouritism; and
- 6.3.4.3. Deliberately omitting or refusing to report or act upon reports of any irregular or dishonest conduct.

## **6.4. Report to the Senior Manager: Security Management**

- 6.4.3. The incident must be reported to the Senior Manager: Security Management as soon as possible after the theft/loss has been discovered.
- 6.4.4. A copy of the sworn affidavit or affirmed statement made to SAPS, must accompany the completed report.
- 6.4.5. In the event of any sensitive/classified documentation or information being stolen/lost this must immediately be reported to the Senior Manager: Security Management, who in turn will report the matter to the National Intelligence Agency for further investigation.

## **6.5. Report to Senior Manager: Risk Management**

- 6.5.3. The Senior Manager: Security Management will forward all the relevant and necessary documentation to the Senior Manager: Risk Management to register the theft/loss and for further investigation and action.
- 6.5.4. The theft/loss will then be reported to the relevant Authority as per Treasury Instructions.

## **6.6. Additional guideline to managers\**

- 6.6.1. The following response steps can serve as an additional guideline to managers when faced with a report of fraud. These should be considered in consultation with the Senior Manager: Risk Management, Senior Manager: Labour Relations.

**Step 1:**

- 1) Evaluate the information or allegation;
- 2) Identify the issues and their implications;
- 3) Consider all possibilities and their implications.

**Step 2:**

- 1) Secure the assets at risk by, for example, notifying banks and other parties holding assets or relevant documentary records.
- 2) Where appropriate, eliminate the immediate threat by suspension or removal of the suspected person from a position of authority by following the applicable process;
- 3) Ensure that all accounting records are secured and back-ups of computer data have been made; and
- 4) Secure the contents of offices where the suspect was employed, such as files and computer data that is the property of the Department.

**Step 3:**

- 1) Start tracing and securing the documentation that was under the control of the suspect; and
- 2) Initiate the investigation process of the alleged fraud.

**Step 4:**

- 1) Start the procedure of recovering of the Department's assets;
- 2) Where appropriate contact the SAPS or other appropriate organisation, for assistance; and
- 3) Audit current accounting procedures and correct any flaws.





- 6.6.2. Managers are also required to ensure that losses or damages suffered by the Department as a result of all reported acts committed or omitted by an employee or any other person are recovered from such an employee or other person if he or she is found to be liable.
- 6.6.3. Where an employee is alleged to have committed financial misconduct the manager, in consultation with the Senior Manager: Labour Relations must ensure that disciplinary proceedings are carried out, within a reasonable period, in terms of the disciplinary code and procedure of Department.
- 6.6.4. The divisional manager and the CFO, with the assistance of any other official, as prescribed in the official delegation of authority, must also ensure that the following steps are taken with regard to financial misconduct in line with the provisions of the Treasury Regulations to the PFMA:
- 6.6.4.1. Ensuring that disciplinary proceedings are carried out in accordance with the relevant prescripts and agreements if an employee is alleged to have committed financial misconduct;
  - 6.6.4.2. Ensuring that disciplinary proceedings are instituted within 30 days from the date of discovery of the alleged financial misconduct;
  - 6.6.4.3. Advising the executive authority, treasury and Auditor-General of any criminal charges laid in respect of the alleged financial misconduct;
  - 6.6.4.4. Advising the executive authority, the Department of Public Service and Administration and the Public Service Commission on the outcome of disciplinary proceedings and/or the outcome of any criminal proceedings;
  - 6.6.4.5. Annually submitting to the Provincial Treasury, National Treasury and Auditor-General a schedule of:

- 6.6.4.5.1. The outcome of any disciplinary hearings and/or criminal charges;
- 6.6.4.5.2. The names and ranks of officials involved; and
- 6.6.4.5.3. The sanctions and any further actions taken against these officials;
- 6.6.4.6. Take the following into account when determining the appropriateness of disciplinary steps against an official in terms of section 38(1)(h) of the PFMA:
  - 6.6.4.6.1. The circumstances of the transgression;
  - 6.6.4.6.2. The extent of the expenditure involved; and
  - 6.6.4.6.3. The nature and seriousness of the transgression;

## **6.7. Reporting losses to SAPS, the HOD and the CFO.**

### **6.7.1. Confidentiality**

- 6.7.1.1. All information relating to fraud that is received and investigated will be treated confidentially.
- 6.7.1.2. The progression of investigations will be handled in a confidential manner and will not be disclosed or discussed with any person(s) other than those who have a legitimate right to such information.
- 6.7.1.3. This is important in order to avoid harming the reputations of suspected persons who are subsequently found innocent of wrongful conduct.
- 6.7.1.4. No person is authorised to supply any information with regard to allegations or incidents of fraud to the media without the express permission of the HOD.

## **6.8. Publication of sanctions**

The HOD will decide, in consultation with appropriate senior managers, whether any information relating to corrective actions taken or sanctions imposed, regarding incidents of fraud should be brought to the direct attention of any person or made public through any other means.

## **6.9. Protection of whistle blowers**

- 6.9.1. An employee who suspects or reports suspected dishonest activity or any such activity that he/she has witnessed may remain anonymous should he/she so require.
- 6.9.2. No person will suffer any penalty or retribution for good faith reporting of any suspected or actual incident of fraud.
- 6.9.3. All managers should discourage employees or other parties from making allegations, which are false and made with malicious intentions. Where such allegations are discovered, the person who made the allegations must be subjected to firm disciplinary, or other appropriate action.

## **6.10. Application of prevention controls and detection mechanisms**

In respect of all reported incidents of fraud, managers are required to immediately review, and where possible, improve the effectiveness of the controls, which have been breached in order to prevent similar irregularities from taking place in future.





## 6.11. Creating Awareness

It is the responsibility of all managers to ensure that all employees, are made aware of, and receive appropriate training and education with regard to this policy.

## 7. ROLES AND RESPONSIBILITIES

- 7.1. The Senior Manager: Risk Management will update the Committee and initiate an investigation into the matter, and consult with Senior Management with regard to steps to follow to resolve the matter. Where appropriate, the matter will be discussed with the Senior Manager: Labour Relations.
- 7.2. All managers are responsible for the detection, prevention and investigation of fraud and must report all incidents and allegations of fraud to the Senior Manager: Risk Management.
- 7.3. It is the responsibility of all employees to immediately report all allegations or incidents of fraud to their immediate manager or, if the employee has reason to believe that his/her immediate manager is involved, to the next level of management.

## 8. MONITORING AND EVALUATION

The Risk Management section shall monitor the implementation of the policy and shall report any deviations to the Head of the Department in writing.





## 9. POLICY REVIEW

The policy shall be reviewed to factor in changes in legal frameworks, organisational development, political and economic trends, and envisaged outputs by the Medium Term Expenditure Framework as well as outcomes of monitoring and evaluation.

## 10. APPROVAL

APPROVED

  
\_\_\_\_\_  
KM MOHASEDI  
HEAD OF DEPARTMENT

DATE : 2010/11/2