

# FRAUD PREVENTION PLAN / STRATEGY 2024/2025



## **public works & roads**

Department:  
Public Works and Roads  
North West Provincial Government  
**REPUBLIC OF SOUTH AFRICA**

## Table of Contents

<b>A: BACKGROUND</b> .....	3
1. INTRODUCTION.....	3
2. REGULATORY FRAMEWORK .....	3
3. FRAUD POLICY STATEMENT .....	4
4. SCOPE OF THE STRATEGY .....	4
5. RESPONSIBILITY OF HEAD OF DEPARTMENT (HOD) AND SENIOR MANAGEMENT TEAM .....	4
6. RESPONSIBILITY OF DEPARTMENT OFFICIALS .....	5
7. APPROACH TO THE DEVELOPMENT OF THE STRATEGY .....	5
8. THE OBJECTIVES OF THE STRATEGY .....	5
9. COMPONENTS OF THE STRATEGY .....	6
<b>B: CREATING AN ETHICAL CULTURE</b> .....	8
10. CREATING AN ETHICAL CULTURE.....	8
11. FRAUD DETECTION INITIATIVES .....	27
<b>C: FRAUD RESPONSE AND RESOLUTION</b> .....	30
12. REPORTING FRAUD AND CORRUPTION .....	30
13. FRAUD AND ANTI-CORRUPTION POLICY AND FRAUD PREVENTION PLAN.....	30
14. INVESTIGATING FRAUD AND CORRUPTION ALLEGATIONS .....	30
<b>D: MONITORING, EVALUATION AND REPORTING</b> .....	32
15. REVIEW OF THE EFFECTIVENESS OF THE FRAUD PREVENTION STRATEGY.....	32
<b>E: COMPLIANCE WITH THE PREVENTION STRATEGY</b> .....	35
<b>F: POLICY REVIEW</b> .....	35
<b>G: APPROVAL</b> .....	35



## A: BACKGROUND

### 1. INTRODUCTION

- 1.1** Fraud and Corruption undermines democratic development, impacting negatively on the performance of public institutions and the optimal use of resources. Ultimately, it denies development and an increased quality of life to the most vulnerable members of society.
- 1.2** The Department has adopted a policy of **zero tolerance towards fraud and corruption**.
- 1.3** Accordingly, this document represents the anti-corruption and fraud strategy for the Department of Public Works and Roads. The Strategy recognises basic fraud prevention initiatives within the Department and takes into account the risks of fraud and corruption as identified in risks assessments performed within the Department. The Strategy addresses fraud and corruption risks at a strategic (Departmental) and at an operational level (fraud risks) level.
- 1.4** The Strategy is intended to set down the stance of the Department towards fraud and corruption as well as to reinforce existing systems, policies, procedures, rules and regulations of the Department aimed at preventing, deterring, detecting, reacting to, and reducing the impact of fraud and corruption, where such dishonest activities exist.
- 1.5** The commitment of the Department to this strategy is for the protection of the public funds it administers and to achieve a reputation for maintaining good systems of internal controls that are determined to prevent and detect all forms of internal and external fraud and corruption committed against the Department.

The Department upholds the principles guiding the conduct of the holders of public service, some of which are:

- Integrity
- Professionalism
- Transparency
- Accountability
- Objectivity
- Respect
- Quality of service delivery and value for money.

### 2. REGULATORY FRAMEWORK

This Plan has been formulated in compliance with the following legislation, regulations and standards:

- Constitution of the Republic of South Africa Act 108 of 1996
- Public Finance Management Act 1 of 1999
- Treasury Regulations Issued in terms of the PFMA
- Protected Disclosure Act 26 of 2000
- Prevention and Combating of Corrupt Activities Act 12 of 2004 (PRECCA)
- Public Service Act 103 of 1994
- DPSA Minimum Anti-Corruption Capacity Requirements
- DPSA Public Service Integrity Management Framework
- Promotion of Administrative Justice Act 3 of 2000



- Promotion of Access to Information Act 2 of 2000
- Prevention of Organised Crime Act 121 of 1998
- National Prosecuting Authority Act 32 of 1998
- Financial Intelligence Centre Act 38 of 2001
- Criminal Procedure Act 51 of 1977
- Protection of Personal Information Act 4 of 2013
- Minimum Information Security Standards Act 68 of 1995
- National Strategic Intelligence Act 38 of 1994
- Public Administration Management Act 11 of 2014.

### 3. FRAUD POLICY STATEMENT

- 3.1 The Department has a **zero tolerance attitude to fraud** and will do everything financially prudent to ensure that fraud, corruption or misconduct, cannot affect its assets and financial well-being.
- 3.2 In keeping with the zero-tolerance approach, acts of fraud, corruption and misconduct will not be tolerated at any level.
- 3.3 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 government.

### 4. SCOPE OF THE STRATEGY

- 4.1 All stakeholders with whom the Department interacts, are expected to abide by the principles contained in the strategy. The Strategy applies to:
- Public servants (Employees of the Department)
  - Suppliers, contractors and providers of goods and services
  - Stakeholders, labour and social societies
  - All other persons with links to the Department.
- 4.2 The strategy relates to all attempts and incidents of fraud and/or corruption, impacting or having the potential to impact on the Department
- 4.3 The strategy will constantly be reviewed to determine its effectiveness, long-term sustainability and alignment to leading best practices. It will continuously evolve as the Department makes changes and improvements in its internal control measures and continuing its drive to promote ethics and prevent fraud and corruption.

### 5. RESPONSIBILITY OF HEAD OF DEPARTMENT (HOD) AND SENIOR MANAGEMENT TEAM

- 5.1 The HOD bears the ultimate responsibility for fraud and corruption risk management within the Department. This includes the coordination of fraud risk assessments, overseeing the investigation of suspected fraud and corruption, and facilitation of the reporting of such instances.
- 5.2 The responsibility of the HOD and Top management is to set the overall tone to reinforce the message that the Department has zero tolerance towards fraud and corruption as well as to:





- Establish an internal control system designed to eliminate or mitigate the fraud risks faced by the Department and management team
- Establish and review a fraud prevention policy, including an appropriate control environment and a fraud response mechanism
- Develop a fraud and ethics risk profile for the Department and regular review of fraud and corruption risks associated with the Department and its processes
- Establish and monitor mechanisms for reporting suspected fraud
- Ensure that staff awareness of anti-fraud and anti-corruption policies is sufficient and that appropriate training is provided on a regular basis
- Ensure timely follow-up action and strengthening of preventative measures. Non-compliance with the requirements of provisions of this Strategy is subject to appropriate disciplinary action.

## **6. RESPONSIBILITY OF DEPARTMENT OFFICIALS**

**6.1** It is the responsibility of every employee to ensure compliance with the Strategy on the basis of zero tolerance towards fraud and corruption within the Department.

**6.2** Each employee shall assist and cooperate in all investigative and preventative activities to prevent, detect and eradicate fraud and corruption, except where such assistance or co-operation is in breach of the official's rights.

## **7. APPROACH TO THE DEVELOPMENT OF THE STRATEGY**

In developing the Strategy, several fraud risks were identified as part of a detailed fraud risk analysis which was undertaken.

However, the risks of fraud addressed in this document should not be relied upon as a definitive list of risks facing the Department, but rather as an indication of the type of risks, bearing in mind the transformation of the risk of fraud resulting from constant technological advancements and changing business processes. The following documents are contained within or attached to the Strategy as they form an integral part thereof:

- Fraud Prevention Policy Statement
- The Code of Conduct
- Gifts Policy
- Remunerative Work Outside the Public Service Policy
- Whistle Blowing Policy
- Ethics Management Policy
- Financial Disclosure Policy

This plan does not guarantee that the Department cannot be impacted by incidents of fraud and corruption but is rather intended to serve as an additional measure to assist in the limitation of fraud and corruption risk with a particular focus on creating awareness, promoting ethical business conduct and to enable the Department to react to instances of fraud and corruption.

## **8. THE OBJECTIVES OF THE STRATEGY**



**2024/25 FRAUD PREVENTION PLAN / STRATEGY**

This plan is intended to set out the stance of the Department towards fraud and corruption as well as to reinforce existing systems, policies, procedures, rules and regulations of the Department aimed at preventing, deterring, detecting, reacting to, and reducing the impact of fraud and corruption, where such dishonest activities exist.

The objectives of the Strategy are to create a culture within the Department which promotes public service and discourages unethical conduct, fraud and corruption by:

- Creating a culture within the Department which is intolerant to unethical conduct, fraud and corruption
- Preventing and detecting unethical conduct, fraud and corruption
- Investigating detected unethical conduct, fraud and corruption
- Taking appropriate action in the event of such irregularities e.g. disciplinary action, recovery of losses and prosecution
- Applying sanctions, which includes redress in respect of financial losses
- Defining and improving accountability, efficiency and effectiveness administration within the Department
- Encouraging all employees and stakeholders to strive towards the prevention and detection of fraud impacting of having the potential to impact on the Department
- Encouraging all officials, stakeholders and the community to report suspicious fraudulent activities without fear of reprisals or recriminations.

**9. COMPONENTS OF THE STRATEGY**

This plan has been formulated based on the approach to mitigating fraud, theft and corruption. The key measures adopted by the Department for preventing, detecting and responding to fraud and corruption are detailed below.

**Fraud Prevention Strategy**

**Prevention**

Preventing the occurrence of fraud, i.e. creating a culture within the Department which is intolerant to unethical conduct, fraud and corruption.

- Code of Conduct for Public Servant (Employees)
- Disciplinary Code and Procedures of the Public Service (Resolution 2 of 1999)
- Chapter 7 of the SMS Handbook for Senior Management Services (SMS)
- Fraud and Ethics Awareness Campaigns
- Ethics infrastructure
- Fraud Risk Assessments
- Recruitment process – Employee Screening
- Obligatory leave periods
- Probation
- Exit procedures and Return of Assets
- Remuneration work outside the public service
- Prohibition of corrupt individuals from the public service
- Naming and shaming of corrupt public servants
- Vendor due diligence
- Review of Supply Chain Management - Conduct of SCM officials in all government institutions
- Proper delegation and segregation of roles within the SCM environment

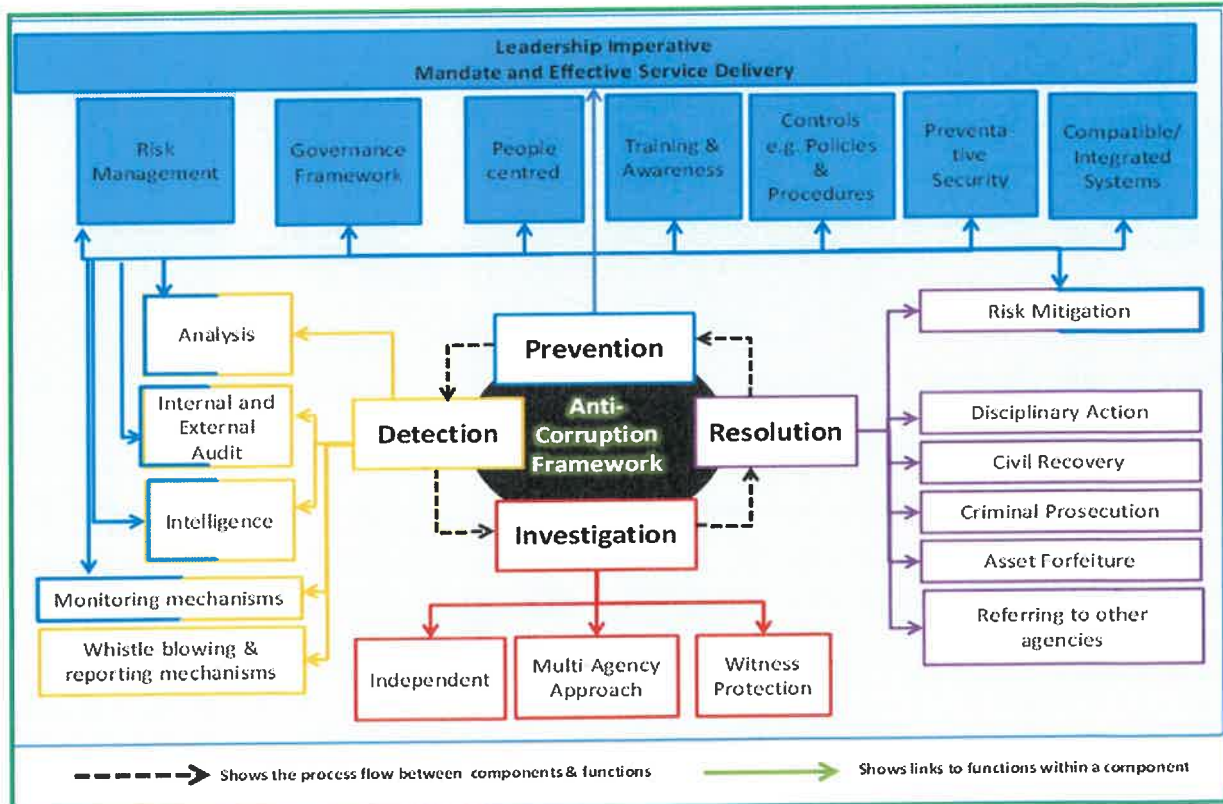


2024/25 FRAUD PREVENTION PLAN / STRATEGY

Fraud Prevention Strategy

	<ul style="list-style-type: none"> <li>• Blacklisting of corrupt suppliers</li> <li>• Conflict of interest disclosures and financial disclosures</li> <li>• Gifts Policy</li> <li>• Internal Control</li> <li>• Physical and Information Security</li> <li>• Security screening of service providers</li> <li>• Vetting of staff</li> </ul>
<p><b>Detection</b>          Detecting existing instances of fraud, i.e. strengthening community participation in the fight against corruption in the Department.</p>	<ul style="list-style-type: none"> <li>• Vigilance by Officials</li> <li>• Internal Audit Function</li> <li>• Forensic data analysis</li> <li>• Whistle-blower Facility</li> </ul>
<p><b>Response and Resolution</b>          Responding to the negative consequences of fraud, i.e. investigating detected unethical conduct, fraud and corruption and taking appropriate actions in the event such irregularities.</p>	<ul style="list-style-type: none"> <li>• Fraud Policy and Response Strategy</li> <li>• Co-operation with other Anti-Corruption Agencies</li> <li>• Disciplinary Enquiry</li> <li>• Criminal Prosecution</li> <li>• Civil recovery.</li> </ul>

An effective fraud prevention strategy integrates the four components of prevention, detection, response and resolution. The graphical depiction below illustrates the fraud prevention model adopted by the Department.



## B: CREATING AN ETHICAL CULTURE

### 10. CREATING AN ETHICAL CULTURE

To reduce the motivation for and rationalisation of fraud and corruption, the Department is committed to creating an ethical culture and to providing guidance to its employees with regards to ethical conduct. Ethical conduct is about distinguishing between what is morally right and wrong with the purpose of doing what is right.

Our employees are expected to fulfill their obligations and conduct themselves to the highest ethical standards, which refer to the moral values and qualities of integrity and honesty. The failure to uphold these standards often gives rise to allegations of corruption and maladministration. The values and principles adopted by the Department are also espoused in Section 195 of the Constitution.

Section 195 (1) of the Constitution reads as follows:

***“Basic values and principles governing public administration.***

*Public administration must be governed by the democratic values and principles enshrined in the Constitution, including the following principles:*

- (a) A high standard of professional ethics must be promoted and maintained.*
- (b) Efficient, economic and effective use of resources must be promoted.*
- (c) Public administration must be development-oriented.*
- (d) Services must be provided impartially, fairly, equitably and without bias.*
- (e) People’s needs must be responded to, and the public must be encouraged to participate in policy-making.*
- (f) Public administration must be accountable.*
- (g) Transparency must be fostered by providing the public with timely, accessible and accurate information.*
- (h) Good human-resource management and career-development practices, to maximise human potential, must be cultivated.*
- (i) Public administration must be broadly representative of the South African people, with employment and personnel management practices based on ability, objectivity, fairness, and the need to redress the imbalances of the past to achieve broad representation.”*

#### 10.1 The Ethical Foundations for Council’s Leadership Responsibilities

The Department’s leadership shall provide effective leadership based on an ethical foundation. Ethical leaders should:

- Undertake their operations with the highest integrity
- Take account of the Department’s impact on internal and external stakeholders
- Ensure that all deliberations, decisions and actions are based on the values underpinning good governance: Responsibility, Accountability, Fairness and Transparency.
- Ethical executive leadership should ensure that the Department is, and is seen to be, a responsible Provincial Department. They should:
- Consider not only financial performance, but also the impact of the Department’s operations on the community and the environment – through more comprehensive integrated reporting
- Protect, enhance and invest in the well-being of communities, the economy and the environment





- Ensure that the Department's performance and interaction with its stakeholders is guided by the Constitution, the Bill of Rights and Batho Pele principles
- Ensure that collaborative efforts with stakeholders are embarked upon to promote ethical conduct and good citizenship
- Ensure that measurable citizenship programmes are implemented
- Ensure that management develops citizenship policies
- Ensure that the Department encourages the participation of communities in its financial management policies.

## 10.2 Understanding Fraud

To understand initiatives for mitigating fraud, theft and corruption, one has to understand what is meant by, and what constitutes fraud, theft and corruption.

## 10.3 Defining Fraud

In South Africa, the common law offence of fraud is defined as "the unlawful and intentional making of a misrepresentation which causes actual and or potential prejudice to another".

The term "fraud" is also used in a wider sense by the general public. In this document the term is used in its widest possible sense and is intended to include all aspects of economic crime and acts of dishonesty (including the legal definitions of fraud, theft and corruption).

In other words, fraud can be described as any conduct or behaviour by a public servant, other external parties, or entity that misleads others into providing a benefit that would normally benefit the public servant, external parties or entity.

## 10.4 Forms of Fraud

Fraud can be perpetrated by:

**Management fraud:** Fraud involving one or more of the members of management is referred to as management fraud. Management fraud may include collusion with third parties outside the Department.

**Employee fraud:** Fraud involving public servants is referred to as employee fraud, but it may include collusion with third parties outside the Department.

**Fraudulent reporting:** Fraudulent reporting involves intentional misstatements or omissions of amounts or disclosures in reports to deceive the users of the report.

Fraudulent events may involve:

- Maladministration or financial misconduct in handling or reporting of money, financial transactions, or other assets
- Incidents of unauthorised, irregular, or fruitless and wasteful expenditure as defined in the PFMA
- Disclosing confidential, proprietary, classified, or restricted information to outside parties
- Irregularly accepting, requesting, offering or giving gifts of material value to or from contractors, suppliers, or other persons providing services/goods to the Department or its Programmes and/or Clients
- Theft of funds, supplies, or other assets.



### 10.4.1 Maladministration

Maladministration is an important manifestation of unethical conduct in the South African public service. Maladministration by a person may be intentional or unintentional and can stem from a practice, policy or procedure. Maladministration means:

- conduct of a public officer, or practice, policy, or procedure of a public authority, that results in an irregular and unauthorised use of public money or substantial mismanagement of public resources or
- conduct of a public officer involving a substantial mismanagement of official functions and includes conduct resulting from impropriety, incompetence or negligence.

Maladministration is to be assessed having regard to relevant statutory provisions and administrative instructions and directions.

#### 10.4.1.1 The definition of maladministration is wide and can include:

- A delay in providing a service
- Incorrect action or failure to take any action
- Failure to follow processes and procedures or the law
- Failure to provide information
- Inadequate record-keeping
- Failure to investigate
- Failure to reply
- Misleading or inaccurate statements
- Inadequate liaison
- Inadequate consultation.

### 10.4.2 Financial Misconduct

The PFMA relates to the regulation of financial management in departments and public entities. It is to ensure that all revenue, expenditure, assets and liabilities of departments and entities are managed efficiently and effectively. It provides for the responsibilities of persons entrusted with financial management in those departments and entities and for connected matters.

Section 38(1) provides that the Accounting Officer/(referred in this document as the HOD) must take effective and appropriate disciplinary steps against any official in the service of the department, trading entity or constitutional institution who has allegedly committed an act of which undermines the financial management and internal control system of the department, trading entity or constitutional institution.

### 10.4.3 Corruption

Corruption in its wider meaning, and as referred to in this Strategy, includes any conduct or behavior where a person accepts, agrees or offers any gratification for him/herself or for another person where the purpose is to act dishonestly or illegally.

Such behavior also includes the misuse of material or information, abuse of a position of authority or a breach of trust or violation of duty.



Fraud and Corruption take various forms. The following are examples of different types of fraudulent or corrupt activities:

- **Bribery** - involves a promise, offering or giving of a benefit that improperly affects the actions or decisions of a public servant.  
*Example: Employee/official in the procurement department accepts a bribe to ensure the awarding of the tender to a specific supplier.*
- **Extortion** - involves coercing a person or entity to provide a benefit to a public servant, another person or an entity in exchange for acting or failing to act in a particular manner  
*Example: A public health official threatens to close a restaurant based on a fabricated health transgression, unless he is provided with regular free meals*
- **Abuse of power** - involves a public servant using her/his vested authority to improperly benefit another public servant, person or entity, or to improperly discriminate against another  
*Example: Promoting a "favourite" employee without following the regulated processes*
- **Conflict of Interest** - involves a public servant acting or failing to act on a matter where the public servant, or another person or entity that stands in a relationship with the public servant, has an interest  
*Example: singling out a specific person/company for award of a contract, or flouting the tender process in order to benefit himself or his partner/relative (who may be the director of the company)*
- **Abuse of privileged information** - involves the use of privileged information and knowledge that the public service possesses as a result of his/her office to provide unfair advantage to another person or entity  
*Example: A public servant gives out privileged information to a friend regarding a contract in which the friend has an interest so that the friend can be awarded the contract.*
- **Favouritism** - involves the provision of services or resources, or the awarding of tenders, by the public servant to favour one supplier ahead of a more deserving supplier  
*Example: Using ethnic, religious, or political grounds to award a contract*
- **Nepotism** - involves giving preferential consideration by a public servant to his/her relative ahead of more deserving persons  
*Example: Appointments of friends, and relatives in posts at the Department*

#### 10.4.4 Theft

A person commits theft if he unlawfully and intentionally appropriates moveable, corporeal or intangible property which belongs to and is in the possession of another.

The following are examples of different types of theft:

- Taking an advance for an official trip, but not going on the trip, then utilising the advance for personal use
- Claiming for subsistence and travel expenditure to attend a course or workshop, and then not attending the course or workshop
- Personal Purchases – the purchase of supplies by public servants under the name of the Department for personal use
- Receiving personal benefits in exchange for assisting a consultant or service provider to gain work at the Department
- Theft of Departmental assets.

#### 10.5 Fraud and Corruption Triggers



For fraud and corruption to occur three factors are relevant. The fraud triangle represents the three fraud and corruption triggers commonly found in fraud events, opportunity, motivation, and rationalisation.



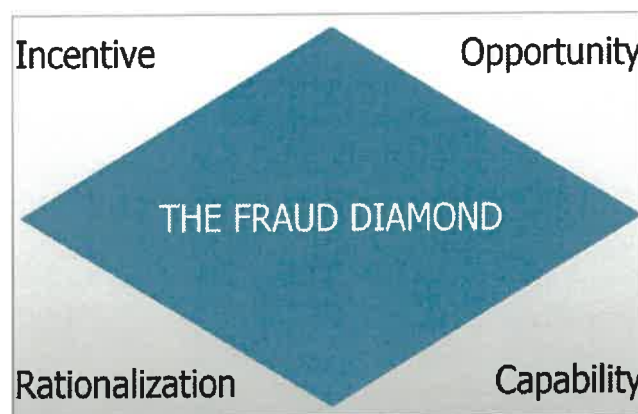
The Department will put in place various controls (a mixture of hard controls and soft controls) to mitigate the risks arising from these three components.

**Opportunity** – refers to the perceived opportunity to perpetrate fraud against the Department e.g. a weak internal control environment, overriding of internal controls, insufficient supervision.

**Motivation** – refers to the perceived need for committing the fraud, e.g. personal debt burden, performance-based compensation.

**Rationalisation** – refers to the frame of mind of the fraudster to justify his/her dishonest act.

The fraud diamond model adds the fourth variable of Capability to three factors shown above. This factor speaks to the belief that the fraud perpetrator must have the necessary traits, abilities, or position of authority to commit the act of fraud.



## 10.6 FRAUD EXPOSURES – FRAUD RISK ASSESSMENTS

In performing the fraud risk assessments, the Department has identified, inter alia, the following fraud risk areas:

- A lack of structured awareness and training programs for employees in applicable policies, procedures, rules, and regulations
- Non-compliance with policies and procedures by employees because of weaknesses in the system for adequately implementing, monitoring and evaluating compliance with policies and procedures.



- Resistance by employees to accept objectives and requirements detailed in strategic strategies and policies and procedures, since they have not been part of the development of the strategic strategies and policies and procedures.
- Theft, abuse or unauthorised use of assets by public servants e.g. Abuse or unauthorised use of vehicles and theft of fuel by public servants.
- Conflict of Interest by public servants and service providers where financial business interests have not been declared.
- Misrepresentation of experience and fabrication of qualifications by candidates during the recruiting process
- Time management:
- Abuse of working hours by public servants performing personal work or being absent during working hours
- Abuse of leave (absenteeism) by officials through not processing leave days taken
- Abuse of Subsistence & Travel claims by claiming for expenses that are not work-related or claiming fictitious claims.
- Ghost employees created on payroll to divert salaries and benefits to existing employees or third parties.
- Lack of document management resulting in unauthorised access to documents, theft and destruction of documents or leaking of confidential information
- The intentional destruction of or unauthorised access (hacking) into the IT infrastructure
- The acceptance of bribes by public servants
- Corporate identity theft – identity used by external parties for fraudulent purposes.
- Favouritism in the award of tenders/contracts

## 10.7 FRAUD RED FLAGS

To understand and to have the ability to detect fraudulent activities, employees should be aware of the behavioural aspects of individuals and organisations. The behavioural aspects of individuals assist in profiling a typical fraudster while that of organisations typifies the risks that make the organisation susceptible to fraud.

### 10.7.1 Individuals

Indicators that individuals may be susceptible to committing fraud include, inter alia, the following:

- Living beyond one's means.
- Sudden change of lifestyle
- Unexplained wealth
- Extensive involvement in speculative investments
- Feeling of being underpaid
- Unusually high personal debts
- Suppliers/ contractors who insist on dealing with only one member of staff
- Severe personal financial losses
- Excessive gambling habits
- Alcohol and drug abuse
- Domestic problems
- Involved in extra-marital relationships.
- Undue family or peer pressure to succeed
- Staff under stress without heavy workload
- Refusal to rotate duties or functions
- Refusing to accept segregation of duties



- Always working late
- Reluctance to take leave
- Refusal to accept promotion
- Dissatisfaction or frustration with job
- Feeling of insufficient recognition for job performance
- Continual threats to quit
- Close associations with suppliers/ contractors
- Close associations with customers
- Poor credit rating
- Rationalisation or justification of poor performance
- Lack of personal stability such as frequent job changes, residence, partners and acquaintances
- High staff turnover, with new staff resigning quickly
- Desire to “beat the system”
- Unreliable communications and reports
- Criminal records
- Undisclosed conflicts of interest.

### 10.7.2 Department

- Indicators that the Department may be susceptible to experiencing fraud include, inter alia, the following:
  - Does not enforce clear lines of authority and responsibility
  - Does not enforce proper procedures for authorisation of transactions
  - Lack of segregation of duties
  - Lack of adequate documents and records
  - A Department that is not frequently reviewed by internal auditors
  - Lack of independent checks
  - No separation of custody over assets from the accounting function
  - No separation of authorisation of transactions from the custody of the related assets
  - Lack of competent personnel
  - Inadequate physical security in Departments, such as locks, safes, fences, keys, cards, etc.
  - Inadequate personnel policies and human resource management systems
  - Failure to maintain records of disciplinary actions
  - Inadequate disclosure of income from external remunerative work
  - Undisclosed conflicts of interest
  - Operating on a crisis basis
  - Operating without budgetary control
  - Budgets not reviewed or meaninglessly justified
  - Too much trust placed in key employees
  - Unrealistic productivity requirements
  - Pay levels not commensurate with responsibilities
  - Inadequate staff - quality and quantity
  - Failure to discipline violators of departmental policies
  - Inadequate communication and awareness about disciplinary codes, fraud policies and codes of conduct



- Absence of conflict-of-interest questionnaires or regular updating thereof
- Inadequate background and reference checks before hiring decisions are made.

## 10.8 FRAUD PREVENTION STRATEGY

### 10.8.1 Fraud Prevention Initiatives

The prevention of fraud and corruption is reliant upon the design and implementation of formal strategies and procedures that minimise opportunities for fraud (so-called "hard controls"), as well as on initiatives aimed at reducing the motivation for, and the rationalisation of fraud (so-called "soft controls"). The initiatives below represent a combination of both hard and soft controls for the prevention of fraud at the Department.

### 10.8.2 Code of Conduct for the Public Servants (Employees)

Section 195(1) (a) of the Constitution requires that "*a high standard of professional ethics must be promoted and maintained*" in public administration generally. In terms of the collective agreement (Public Service Coordinating Bargaining Council Resolution 2 of 1999) all the employees in the Public Service have the responsibility to comply with the prescribed Code of Conduct, as promulgated by the Public Service Commission.

- The Code of Conduct was developed in order to set down clear guidelines to employees as to what is expected of them from an ethical point of view, both in their individual conduct and in their relationships with others.
- The Code is applicable to all employees of the Department
- The Code of Conduct requires the following proactive prescripts:
  - Employees are to refrain from favouring relatives and friends in work-related activities and never abuses his or his authority or influences another employee, nor is influenced to abuse his or her authority.
  - Employees shall not engage in any transaction or action that is in conflict with or infringes on the execution of his or her official duties.
  - Employees will recuse himself or herself from any official action or decision-making process which may result in improper personal gain, and this should be properly declared by the employee.
  - Employee shall not, accept any gifts, benefits or item of monetary value (a description and the value and source of gift from any person for himself or herself during the performance of duties as these may be construed as bribe.
  - Employee shall not, without approval, undertake remunerative work outside his or her official duties or use office equipment for such work.
- In order to improve ethical conduct of its officials and create awareness of the Code, the Department will undertake the following steps:
  - The Code of Conduct will be circulated to all officials and included in the induction packs of new officials.
  - The Department will provide training on the Code by conducting workshops and awareness presentations and communication programmes in order to create an understanding of the Code and to reinforce the expectation of the Department with regard to the ethical behaviour and integrity.
  - All officials will be required to sign an annual declaration evidencing their understanding and commitment to and compliance with the Code.



### 10.8.3 Disciplinary

- a) The Disciplinary Code and Procedures of the Public Service (Resolution 2 of 1999) for levels 1 to 12 and Chapter 7 of the SMS Handbook for Senior Management Services (SMS) set out the appropriate steps to be undertaken to resolve disciplinary matters.
- b) The Department acknowledges that the consistent and efficient application of disciplinary measures is integral to the success of the Strategy. In order to ensure the consistent, ethical, efficient and effect application of disciplinary measures, the Department will undertake the following steps:
  - Conduct ongoing awareness presentations and communication programmes on the content of the Disciplinary Policy to ensure that all respective Managers understand the standards of discipline, the procedure for the application of disciplinary measures and the disciplinary process.
  - Developing a mechanism whereby Managers are held accountable for the management and addressing of misconduct within their business units.
  - Developing a monitoring system in order to keep proper records of all disciplinary actions taken thereby facilitating the consistent application of disciplinary measures.

### 10.8.4 Fraud and Ethics Awareness Campaigns

The Department will provide appropriate fraud prevention training in specific areas where the Department deems a high residual risk of fraud, theft or corruption exists. The training will serve not only to highlight unethical and unacceptable business conduct and the resultant disciplinary action, but also to reiterate the Department's shared core values and the impact these values have on the employees' day-to-day operations.

In this regard, public servants will, on an ongoing basis, receive training on the following:

- Fraud prevention strategy and fraud response strategy and the public servants' responsibilities to mitigate/reduce risk of fraud and misconduct
- Code of conduct
- Disciplinary Code
- Specific policies within the Department (i.e. gifts or conflicts of interest)
- Procedures available to public servants to seek advice and report suspected misconduct
- Latest fraud trends
- Relevant regulatory requirements
- Manifestations of fraud and corruption in the workplace
- The importance of ethics within the Department and the consequences (for individual public servants, but also for the Department as a whole) of unethical conduct
- Identifying ethical dilemmas, fraudulent and corrupt behaviour and strategies for resolving ethical dilemmas
- Presenting case studies which will assist in developing behaviour to articulate and encourage attitudes and values which support ethical behaviour
- Communicating the implications of unethical behaviour and its impact on individuals, the workplace, professional relationships within the Department and external stakeholders
- How to report fraud and corruption.

The frequency of training and communication will also be at induction, on an annual basis and as and when deemed necessary. Training will be provided through formal/informal meetings.





The following methods of communication will be considered, amongst others:

- E-mails/ad hoc internal fraud alerts
- Intranet postings
- Regularly running awareness campaigns on fraud and ethical conduct
- Publicising “Lessons Learned” out of investigations into allegations of fraud and corruption amongst public servants
- Circulating success-related fraud modus operandi within the Department’s environment;
- Placing notices or other communiques related to fraud prevention and detection in strategic areas to which public servants and the public have access
- Developing a fraud prevention suggestion box where all public servants could make suggestions on how to prevent fraud and corruption.

### 10.8.5 Fraud Awareness with Stakeholders

The Department will also implement various means of communicating the fraud prevention initiatives, including the following:

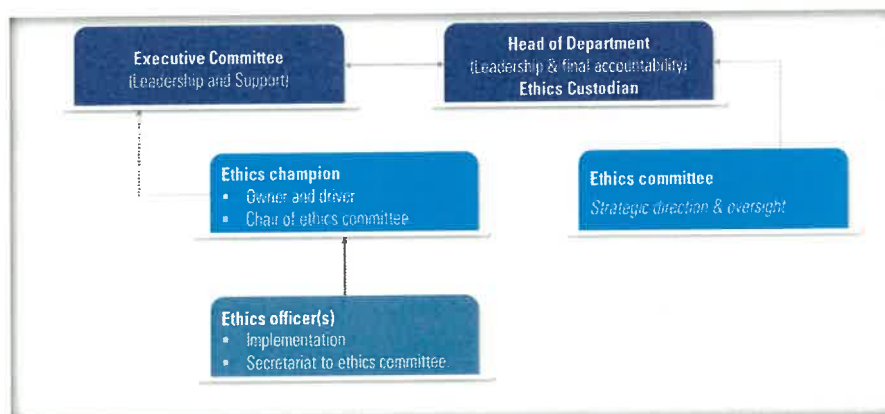
- Developing a poster campaign aimed at all stakeholders to popularise the Department’s stance against fraud and also its expectations with regards to ethics and integrity of all stakeholders
- Circulating appropriate sections of the Code of Conduct to other stakeholders, i.e. consultants and contractors
- Giving copies of the Code of Conduct to suppliers of goods and services
- Using the local paper to communicate issues relating to the prevention and detection of fraud, including matters reported and action taken.

### 10.8.6 Ethics Infrastructure

The Public Sector Integrity Management Framework (PSIMF) has been introduced to provide a comprehensive Integrity Framework derived from the existing regulatory framework in order to align all measures regulating ethics and integrity in the public sector, with the following objectives:

- Strengthening existing measures regulating probity in the public service;
- Strengthening capacity to prevent corruption;
- Monitoring and evaluation to ensure compliance; and
- Enforcement as a deterrent.

The PSIMF provides the following guideline in respect of the Ethics Infrastructure within the Department:



Accordingly, the Department shall consider:

- Designating an Ethics Champion at executive level with the delegated authority to drive ethics and anti-corruption initiatives;
- Establishing an Ethics Committee (or make use of an existing committee) to assist the determination of the Department's ethics strategy, and to provide oversight of integrity management;
- Establishing an Ethics Office. It is a dedicated structure, positioned at a high level, responsible for day-to-day-work related to the ethics management programme. Functions will include: overall oversight of ethics programme, advice and reporting, investigation, monitoring and audit, corporate social responsibility/integrity function;
- Appointing Ethics Officer(s) and assign them the following responsibilities:
  - Promote integrity and ethical behaviour in the Department
  - Advise public servants on ethical matters
  - Ensure integrity of the Department's policies, procedures, and practices
  - Identify and report unethical behaviour and corrupt activities to the HOD
  - Manage conflicts of interest, including:
    - Financial disclosures of public servants
    - Application for external remunerative work
- Keeping a register of all public servants under investigation and those disciplined for unethical conduct
- Developing and implement awareness programmes to educate officials on ethics, good governance, and anti-corruption measures.

### 10.8.7 Fraud Risk Assessments

The Department acknowledges the fact that it faces diverse business risks from both internal and external environments.

At Fraud Risk Assessment workshops, the potential risks are assessed and prioritised. After identifying the major risks, the team designs methods of preventing fraud in these areas. Risk owners are identified and the results of the fraud risk assessment are documented in a Fraud Risk Register, which is maintained by internal audit and forms part of its reporting to the Audit Committee and other senior executives.

Proposed action may also be developed in relation to risks assessed as being of a lower level of residual risk. All actions proposed by the risk assessment team will be evaluated by senior management, as appropriate, prior to implementation of treatment plans.

The above will be formulated into a Fraud and Ethics Risk Register, which will prioritise the fraud and corruption risks and indicate actions to mitigate these risks.

Annually, management presents these revised risks with mitigating techniques to the Audit Committee for consideration. The risks that are both inadequately managed and carry material risk in the current environment are addressed, as new systems are required. The assessments will be completed annually, and internal audit needs to assess the effectiveness of the controls.

The 2025/26 fraud risk assessments will be conducted during the 2024/25 financial year. The following rating scales will be applied when conducting the fraud assessments:



**Likelihood Rating Scale:**

Descriptor	Level	Definitions
Rare	1	Fraud is conceivable but is only likely to occur in extreme circumstances
Unlikely	2	Fraud may occur infrequently and is unlikely to occur
Moderate	3	There is an above average chance that fraud will occur
Likely	4	Fraud could easily occur
Common	5	Fraud is already occurring

**Impact Rating Scale:**

Descriptor	Level	Definitions
Insignificant	1	There is 90 - 100% that the controls will prevent fraud. (Unacceptable - Action must be taken)
Minor	2	There are 70 - 89% chances that it is likely that the controls will prevent fraud. (Unacceptable - Action must be taken)
Moderate	3	There are 50 - 69% chances it is likely that the controls will prevent fraud. (Unacceptable - Action must be taken)
Major	4	There are 30 - 49% chances that it is likely that the controls will prevent fraud risks. (Unacceptable - Action must be taken)
Critical	5	There is 1 - 29% chance that it is likely that the controls will prevent fraud. (Unacceptable - Action must be taken)

**Control Effectiveness Rating Scale:**

Descriptor	Effectiveness Rating	Definition
Very Good	5	The controls in place are working at an optimum level
Good	4	The controls in place are addressing the risks, but are not working at an optimum level
Satisfactory	3	The controls in place are working at an acceptable level, but more can be done to strengthen these controls
Weak	3	The controls in place need to be strengthened or new controls need to be implemented
Unsatisfactory	1	The controls in place are ineffective, and new controls need to be implemented



**Residual Risk Exposure**

Risk rating	Risk magnitude	Response
20 - 25	Maximum	Unacceptable - Action must be taken immediately – considering zero tolerance stance to fraud
15 - 19	High	Unacceptable- Action must be taken – considering zero tolerance stance to fraud (Major level of control intervention)
10 - 14	Medium	Unacceptable - Action must be taken – considering zero tolerance stance to fraud (Moderate level of control intervention)
5 – 9	Minimum	Unacceptable- Action must be taken – considering zero tolerance stance to fraud (Update routine control procedures)
1 – 4	Low	Unacceptable- Action must be taken – considering zero tolerance stance to fraud (Update routine control procedures)

**10.8.8 Human Resource Policies and Systems**

The Department undertakes to develop human resources systems, policies, and procedures corporate the promotion of integrity, anti-fraud and anti-corruption practices as detailed below:

- Recruitment - Employee Screening Procedures

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 Human Resource Department and withdraw from any further procedures.

Should it be subsequently identified that a person involved in the decision-making elements of the recruitment process has a relationship with the potential employee and has not declared the potential conflict, that person may be subject to disciplinary procedures.

Members serving on the Selection and Short-listing committee shall be bound by the Confidentiality and Conflict of Interest Disclosure clauses.

- Pre-employment Screening

Vetting and screening are some of the simplest and most effective practices to incorporate within the Department. By consistently applying these practices, the Department will prevent many corruption and labour issues and contribute to high standards of professional ethics in departments.

Pre-employment screening will be carried out in accordance with the Department’s recruitment strategy, and evidence of such screening will be maintained by the HR Department.





- Employee Induction Training

Induction training offers an opportunity to establish clear foundations and expectations in terms of ethics, integrity, fraud awareness, fraud prevention and other concepts that are the foundation of all accountable institutions.

All new officials have to go through the induction programme. The Department will ensure that Department's Fraud Prevention Strategy, Code of Conduct and Ethics, Disciplinary Code and Fraud awareness training is incorporated.

This training will be done systematically and is generally the responsibility of the Corporate Services to ensure that the new officials undergo induction training in the first three months of commencing work. Contractors and temporary public servants will also be considered for the induction training.

- Obligatory Leave Periods

In order to reduce the risk of over-worked public servants who could become careless, leading to non-compliance with internal controls, and to reduce the risk of fraud, officials are allowed to take a minimum of 22 days of annual leave. This should include an annual compulsory period of 10 consecutive leave days.

The Department Heads of Department will be encouraged to ensure that appropriate controls, e.g. appropriate scrutiny, and supervision are put in place in instances where, for extended periods of time, public servants do not take leave due to work commitments.

- Probation

Compulsory probationary periods should be applicable to all full-time officials. Relevant vetting will be implemented for officials on probation, during probation and prior to their final appointment, in view of the long duration of the probationary period.

- Exit Procedure and Return of Assets

The exit procedure and return of assets, if not properly addressed, could lead to losses for the Department.

The exit procedure at the Department requires the official to return all assets and to complete the exit clearance form as well as the attendance of an exit interview. This includes securing all electronic information of the official.

Furthermore, all officials will be required to complete an employee "exit interview questionnaire" upon resignation from the Department. Any suspected fraud, corruption or misconduct identified through this process will be communicated to Senior Management for investigation. This is necessary to ensure that factors contributing to misconduct and fraudulent activity by the public servants can be managed as a process to mitigate fraud risk.



- Remunerative Work outside the Public Service

When outside business/directorships are being considered, prior written approval must be obtained from the MEC responsible for the Department.

In considering an application for outside remunerative work, MEC or designated official shall, in addition to the current criteria, assess whether the outside work could reasonably interfere with or impede the effective and efficient performance of the employee's functions.

The MEC shall consider the following aspects when assessing the application:

- The nature and extent of work to be undertaken
- The time required for the outside work
- The employee's performance record.

The current period for considering an application for outside remunerative work shall be extended from 30 to 60 days to give the Executive Authority enough time to assess the implications of applications for outside work.

- Prohibition of Corrupt Individuals from Public Service

Public servants that have been party to acts of corruption, often change employer within the public sector. To remedy this situation and to raise the integrity and ethics of the public service and the businesses it does business with, prohibition must be established by:

- Excluding an employee and owners and directors of businesses found criminally guilty of corruption from employment or contract with the public sector for a maximum period of 5 years. The presiding officer has discretion as to the period of the prohibition
- Recording the prohibition of such persons on employment systems
- Publication of sanctions and names of businesses, owners and directors
- Requiring institutions to consult the centralised electronic register before contracts are concluded
- Requiring contractors to declare previous criminal convictions related to corrupt practices.
- The Department will consider the possibilities of naming and shaming public servants involved in fraud and corruption.

- Procurement Policies and Procedures

The Department is committed to developing and maintain supply chain management policies and procedures which will incorporate the fraud and corruption prevention initiatives, as outlined below:

- Vendor Due Diligence Procedures

The following due diligence procedures will be considered. All suppliers need to be registered on the database. The due diligence should be initiated, and is should be ongoing.

The following procedures may be performed:

Level 1	One-time vendors, low volume/value vendors (excluding sensitive vendors)	<ul style="list-style-type: none"> <li>- CIPC company registration check</li> <li>- Valid Tax Clearance certificate</li> <li>- Desktop-based search for online presence, negative media publicity</li> <li>- Desktop-based search for litigation check</li> <li>- National Treasury Blacklist database check</li> <li>- Security vetting of service provider</li> <li>- Signing of confidentiality agreement with service provider</li> </ul>
Level 2	Medium volume/value vendors (excluding sensitive vendors)	<ul style="list-style-type: none"> <li>- CIPC company registration check</li> <li>- Valid Tax Clearance certificate</li> <li>- Desktop-based search for online presence, negative media publicity</li> <li>- Desktop-based search for litigation check</li> <li>- National Treasury Blacklist database check</li> <li>- Security vetting of service provider</li> <li>- Signing of confidentiality agreement with service provider</li> <li>- Site visits</li> </ul>
Level 3	High volume/value vendors including sensitive vendors	<ul style="list-style-type: none"> <li>- CIPC company registration check</li> <li>- Valid Tax Clearance certificate</li> <li>- Desktop-based search for online presence, negative media publicity</li> <li>- Desktop-based search for litigation check</li> <li>- National Treasury Blacklist database check</li> <li>- Security vetting of service provider</li> <li>- Signing of confidentiality agreement with service provider</li> <li>- Site visits</li> <li>- Ultimate Ownership check.</li> </ul>

Declarations are also requested from the vendor regarding:

- Any potential conflict of interest due to the expected relationship; whether there exists any relationship between the vendor/vendors and public servants
- On an annual basis, declarations are requested to be resubmitted by the vendors
- All such declarations may be reviewed to identify potential risks to the Department



- Blacklisting of Corrupt Suppliers

An integral strategy towards effective supply chain management is not to award contracts to persons with a history of abuse of the supply chain management system. Prior to awarding any contract, the HOD is required to check the prohibition status of the recommended bidder.

If they are listed, the contract cannot be awarded. The HOD is empowered to restrict companies or persons from doing business with the public sector for a period not exceeding 10 years, if such companies or persons have obtained preferences fraudulently or failed to perform on a contract based on the specified goals.

Any restriction imposed by the HOD must be forwarded to the National Treasury for loading onto the central List of Restricted Suppliers.

A central List of Restricted Suppliers must be established containing details of companies or persons that have been restricted from doing business with the public sector.

- Conflicts of Interest Policy

A conflict of interest exists when officials have a direct or indirect personal interest that could interfere or be perceived by others to interfere with their objectivity in the performance of their duties. It includes using an employee's position, confidential information, work time, or the Department's materials or facilities for private gain or advancement. A conflict may occur when an interest benefits any member of the employee's family, friends, or business associates.

Public servants are required to support and advance the interests of the Department, which is in direct service of the public. Officials should therefore avoid placing themselves in situations where their personal interests conflict or potentially conflict with the interests of the Department or the broader interest of the public. All officials (and their immediate families) are prohibited from being directly or indirectly associated with any business entity that provides goods and services to the North West Provincial Government.

All officials are required to disclose their business interests annually and this should be updated routinely as and when the individual's circumstances change.

In line with the above, the Department has adopted a Conflict-of-Interest Policy in order to address both the acceptance and offering of gifts by all employees of the Department.

- Types of Conflicts of Interest:

The following constitute conflicts of interest and should be avoided and/or declared by the official:

- Part-time employment in areas similar to those in which the Department is involved
- External work for suppliers, vendors, or other organisations hired by the Department or that derive benefit from the Department
- A financial interest, such as a shareholding or a commission position, in a business that is a supplier to the Department
- Exclusive or preferential discounts from an employee or representative of a supplier, person under investigation, or member of the public, including the purchase of shares from a supplier on a preferential basis





- Dealing directly with or through a spouse or family member who is a supplier or vendor, or is employed by one
  - Nepotism or favouritism in hiring; appointment of family members to a position within one's influence
  - Soliciting loans from a citizen, a person under investigation, or a supplier, that is not generally in the business of granting loans to the public
  - Giving work time and Department assets to external interests, including political campaigns, business issues, and personal matters
  - Participation in any activity that might lead to the disclosure of proprietary information of the Department or of citizens who have entrusted this information to the Department.
- Disclosure of Financial Interest and Assets

The requirement to disclose financial interests shall be extended to all public servants in the Department through the following:

- Provisions for the compulsory declaration of actual and/or potential conflicts of interest both by suppliers and employees of the Department concerned dealing with these suppliers.
- An official whose spouse, partner, business associate or close family member, stands to acquire any direct benefit from a contract concluded with the Department, shall disclose in writing full particulars of the benefit to the Ethics Officer and withdraw from participating in any manner whatsoever in the process relating to that contract.
- An electronic submission (edisclosure) of financial disclosures has been implemented in the Public Service Act and public servants shall disclose every time new registrable interests are obtained.

**Disclosure of Financial interest and Assets**

<i>Heads of Department and Senior Management</i>	Senior management are required to disclose their financial interest and assets by 30 April annually or on appointment as the case may be and whenever their financial interest change.
<i>All public servants</i>	All public servants including those public servants on an Occupational Specific Dispensation (OSD) in the Administration are required to disclose their financial interest and assets by the prescribed due date issued by the DPSA in the Disclosure Framework or on appointment, as the case may be and whenever their financial interest change.

**Declaration of relatives doing business with Government**

<i>All public servants</i>	Public servants are required to declare whether they have relatives who are doing business with government, particularly the Local Administration.
----------------------------	--

If public servants become aware of, or suspect a contravention of the Conflict of Interest, they must report this immediately to their line manager, Human Resources Manager or Internal Audit/ Risk Management. The extension of compulsory declaration of interest to lower ranks should be implemented.



- Compliance with the Conflict of Interest and Financial Disclosure Framework

The declaration of interest form should accurately reflect companies, close corporations, partnerships or associations of which officials may be a director or in which public servants may have a financial interest. Human Resources will be required to perform checks on all disclosures declared and maintain the consolidated register.

Failure to disclose potential conflicts of interest will be dealt with in terms of the Disciplinary Code and Procedures for the Public Service and/or prosecuted criminally as the case may be.

- Gifts and Hospitality Policy

It is a common perception that officials employed within the Department face the greatest challenge to their integrity in the form of enticement to accept bribes from unethical suppliers, contractors and consultants. Furthermore, these trading partners are also often viewed as untrustworthy in-service delivery.

- Officials must as a general rule not accept gifts where the gift has been given because of the giver's official relationship with the administration itself.
- Management and staff should recognise that accepting a gift, entertainment, hospitality, or a gratuity from suppliers or other parties may infringe on their responsibility to provide objective, impartial decision-making. A clarification of these terms may help discourage abuse:
  - Gifts are items and services of value, which are given by outside parties, e.g. money, computers, cars etc. Any of the following can also be considered gifts:
    - Entertainment is provided for the purpose of relaxation and recreation provided by outside parties, e.g. tickets to sporting events, holidays etc.
    - Hospitality is provided to look after a human need or to display respect to a person or a group, e.g. extravagant meals, accommodation etc.
  - Gratuities are rewards or incentives provided in exchange for or in recognition of the completion or delivery of work, a product, or an achievement. This includes any of the above seemingly given as a thank-you.
  - Kickbacks include anything of value provided directly or indirectly for the purpose of improperly obtaining or rewarding favourable treatment. In the wrong circumstances any of the above can be construed as a kickback.
  - Donations are charitable contributions to a cause.

In line with the above, the Department has adopted a Gifts Policy to address both the acceptance and offering of gifts by all employees of the Department.

- Internal Controls

The systems, policies, rules and regulations of the Department prescribes various controls, which, if effectively implemented, would limit fraud. These controls may be categorised as follows:

- Authorisation Controls: All transactions require authorisation or approval by a responsible person with appropriate authority limits. The authority limits are specified in the Delegation of the Department.



- Physical Asset Controls: This relates to Custody of Assets and involves procedures and security measures designed to ensure that access to assets is limited to personnel who have been duly authorised in writing.
- Segregation of Duties: Placed in context of fraud, segregation of duties lies in separating either the authorisation or the custodial functions from the checking function. Segregation of duties reduces the risk of intentional manipulation or error and increases the element of checking. Functions that should be separated include those of authorisation, executions, custody and recording, and, in the case of computer-based accounting, system development and daily operations.
- Supervision Controls: This control relates to supervision by managers of day-to-day transaction and the recording thereof.
- Management Information: This relates to the management of accounts and budgetary controls.

To ensure that these internal controls are effectively and consistently applied, deficiencies and non-compliance identified by internal audit will be addressed as follows:

- The Department will constantly encourage Managers to recognise that internal control shortfalls are symptoms of potential fraud and Managers should therefore strive to identify and address the causes of these internal control weaknesses.

Where managers do not comply with basic internal controls i.e. non-adherence to the Delegation of Authority limits, firm disciplinary action will be considered. All officials are encouraged to be aware of and to identify any internal control weaknesses to their manager or in the case of manager, to the Head of Department or alternatively to the relevant reporting authority.

- Physical and Information Security

Control over physical and information security is central to this Strategy. In addition, Departments are often the custodians of sensitive information belonging to the public that it serves. The implications of poor control over this information could seriously undermine the Strategy, and therefore Department policies on security of information must be implemented and guarded with the highest standards of integrity.

The Department will take the following steps to improve physical security and access control at its offices:

- Officials will be sensitised on a regular basis to the fraud and corruption risks associated with information security and the utilisation of computer resources (in particular - access control) and the Department will need to ensure that systems are developed to limit the risk of manipulation of computerised data
- Regular communiques will be forwarded to officials emphasizing the contents of the IT Policy and security policies, with a particular emphasis on e-mail and Internet usage, and the implications (e.g. disciplinary action) of abusing these and other computer-related facilities.

## **11. FRAUD DETECTION INITIATIVES**

The Department aims to detect instances of fraud effectively and swiftly, thereby ensuring prompt action and minimising possible losses.



Detection of fraud and corruption may occur through:

- Vigilance by Officials
- The Internal Audit function
- Application of Forensic Data Analysis techniques
- Whistleblowing reports
- Instituting and implementing an effective and conducive control environment.

### 11.1 Vigilance by Officials

The Department expects all people and organisations that are in any way associated with it to conduct their activities in an honest and fair manner and to lead by example.

In so doing, all officials are encouraged to be aware of and to identify any internal control weaknesses within the working environment and to communicate such weaknesses to their Manager, or in the case of Manager, to the HOD or alternatively to the relevant reporting authority.

### 11.2 Internal Audit Function

A robust internal audit programme, which focuses on the prevalent high fraud and corruption risks, should be introduced to serve as an effective preventative measure in terms of detecting control deficiencies prior to a fraud event occurring.

The internal audit programme will cover the following:

**Surprise Fraud Audits:** Unplanned fraud audits conducted on specific business processes throughout the year. Internal Audit will consider the following in determining which business processes to audit:

Key risk areas as identified via fraud risk assessments:

- Recent risk exposures
- Recent forensic investigations
- Long outstanding management actions.

**Post-fraud Reviews:** A review of fraudulent transactions after they have been processed and completed can be effective in identifying other similar fraudulent or corrupt activity.

In addition to the possibility of detecting further fraudulent transactions, such a strategy can also have a significant fraud prevention effect as the threat of detection may be enough to deter a staff member who would otherwise be motivated to engage in fraud and corruption. The Internal Audit Unit will be responsible for implementing an internal audit programme which will incorporate steps to ensure adherence to internal controls to mitigate fraud and corruption.

### 11.3 Forensic Data Analysis

Fraud will be addressed by conducting reviews in order to secure a more detailed understanding of the areas wherein these risks exist. The following are examples of a selection of tests on data that may assist in identifying irregularities:

- Officials with false ID numbers
- Officials that are linked to companies or CC's
- Officials linked to suppliers of the Department
- Suppliers with shared information, similar names or false VAT numbers
- Payments made over weekends or on public holidays





- Invoices in number sequence, duplicate invoices or payments
- User trends (spikes in usage)
- Splitting of orders (3 invoices to stay under thresholds)
- Round amount payments and contracts or payments close to threshold and or delegations.

Furthermore, specific transactions will be selected in order to conduct fraud detection reviews, including fraud susceptibility assessments, aimed at detecting possible incidents of fraud and/or control weaknesses in order to address these:

- Weaknesses in internal controls
- Weaknesses in the payroll system
- Weaknesses in information technology and processing systems
- Weaknesses in Human Resources Management development policies
- Weaknesses in budget management and reviews and financial reporting
- Collusion in tendering and procurement
- Fraud relating to fleet management (e.g. abuse of vehicles and petrol cards)
- Abuse of assets, including computer equipment
- Poor inventory and asset management

#### 11.4 Whistle-blower Facility

The Protected Disclosures Act 26 of 2000 (PDA), also known as the Whistle-Blower Act, makes provision for public servants to report unlawful or irregular conduct by employers and fellow public servants, while providing for the protection of public servants who 'blow the whistle'. The PDA makes provision for the following:

- Public servants to report unlawful or irregular conduct by employers and fellow public servants
- Protection of public servants who blow the whistle from "occupational detriment" by employers when making certain protected disclosures
- Any employee who has information of fraud, corruption or other unlawful or irregular action(s) by his/her employer(s) or co-public servants to report such actions, provided that he/she has evidence that:
  - A crime has been, is being, or is likely to be committed by the employer or employee(s)
  - The employer or public servants has/have failed to comply with an obligation imposed by law
  - A miscarriage of justice has occurred or is likely to occur because of the employer's or employee's actions
  - The health or safety of an individual has been, is being, or is likely to be endangered
  - The environment has been, is being or is likely to be endangered
  - Unfair discrimination has been or is being practised
  - Any of the above has been, is being, or is likely to be concealed.

The Department recognises that in order to effectively prevent fraud, all fraudulent activities detected by officials and other stakeholders should be reported and investigated.

The Department will continue to support the National Anti-Corruption Hotline of the Public Service Commission and encourages its officials to utilise this service to supply information relating to fraudulent activity. The Fraud Hotline is also an integral mechanism for the reporting of fraud in terms of the fraud policy. The **National Anti-Corruption Hotline number is 0800 701 701.**



## C: FRAUD RESPONSE AND RESOLUTION

### 12. REPORTING FRAUD AND CORRUPTION

Allegations of fraud, corruption, maladministration, theft, mismanagement of funds and misrepresentations may be received through:

- Anti-corruption hotline
- Whistle-blowers
- Executing authorities
- Senior management of government institutions
- Normal assurance reviews.

The Department encourages all public servants to report any incidents of fraud and corruption through the **National Anti-Corruption Hotline** whereby public servants can report fraud without fear of reprisal or victimisation by fellow public servants.

### 13. FRAUD AND ANTI-CORRUPTION POLICY AND FRAUD PREVENTION PLAN

The Department has developed a **Fraud and Anti-Corruption Policy and Fraud Prevention Plan** which contains provisions for the reporting of allegations of fraud. The Fraud Prevention Plan sets out the Department's stance on Fraud and Corruption as well as the response mechanisms in place to report, investigate and, resolve incidents of fraud and corruption impacting the Department.

### 14. INVESTIGATING FRAUD AND CORRUPTION ALLEGATIONS

If fraud or corruption is detected or suspected, the Department, depending on the nature of the concern, will initiate investigations. The Department should consider the following to respond to the fraud or corruption:

- Forensic investigation
- Internal disciplinary enquiry
- Criminal prosecution
- Civil recovery of losses.

#### 14.1 Forensic Investigations

All investigations performed and evidence obtained will be in accordance with acceptable practices and legal requirements. The 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 findings of the investigation.

#### 14.2 Disciplinary Enquiry

In instituting an internal disciplinary enquiry against a public servant, the Department must ensure that all disciplinary proceedings take place in accordance with the procedures as set out in the organisation's Human Resources Policy and Manual or disciplinary code.



The ultimate outcome of disciplinary proceedings may involve a person/s receiving written warnings or having their services terminated.

The Department must:

- Insist on disciplinary proceedings against corrupt officials
- Make public statements against corruption and corrupt officials in press statements, newsletters, circulars, etc.
- Lay criminal charges against internal and external perpetrators
- List corrupt and poor-performing suppliers on the List of Restricted Suppliers
- Recover the Department's losses and cancel the contracts.

### **14.3 Criminal Prosecution**

In the event that fraud, theft or corruption was detected, investigated, and warranted disciplinary proceedings, prosecution or action aimed at the recovery of losses will be initiated and the matter will be reported to the SAPS, regardless of the value of the offence. All cases should be reported to the National Treasury, the relevant provincial treasury and the Auditor-General as contemplated in Section 85 of the PFMA.

The Special Investigating Unit (SIU), can assist the Department with internal investigations. Cases are referred to the SIU by Presidential Proclamation. The Department can request for this to be issued where they require the services of the SIU.

### **14.4 Civil Recovery**

Where there is evidence of fraud or corruption and there has been a financial loss to the organisation, action 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.

The Prevention of Organised Crime Act of 1998 ("POCA") makes provision for property tainted by criminal activity to be forfeited to the state by way of a civil action. Commonly called civil asset forfeiture, this allows the state to confiscate suspected criminals' assets purely through a civil action against the property, without the need to obtain a criminal conviction against the owner of the property.

The Asset Forfeiture Unit was created to serve as a dedicated unit to build up the necessary expertise to deal with the complexities of forfeiture and whose performance is measured solely in terms of forfeiture.

In terms of section 300 of the CPA, the Court may award compensation where the committing of an offence has caused damage to or loss of property to any person or Department. On the conviction of any person, the court can be requested to make the section 300 restitution part of the court order. Such an order has the same force as a civil order. The benefit of using this mechanism is that it comes without any legal fees and is driven by the State Prosecutor.

Any Department that has suffered financial losses due to corrupt or fraudulent behaviour by officials should pursue the possibility of recovering some or all of its losses from the perpetrator's pension or provident fund. In terms of section 37D (b) (ii) of the Pension Funds Act (24 of 1956), the employer may recover compensation in respect of any damage caused to the employer by reason of any theft, dishonesty, fraud or misconduct by the member, and in respect of which:

- The member has in writing admitted liability to the employer
- Judgment has been obtained against the member in any court, including a magistrate's court.

The Department must therefore either obtain a cession of the Pension Fund benefits by the employee, or supply the relevant Pension Fund with a court judgment indicating its entitlement. The judgment may either be obtained through a civil claim procedure or a Section 300 ruling in terms of the Criminal Procedure Act.



## D: MONITORING, EVALUATION AND REPORTING

Any employee who fails to comply with the requirements of provisions of this Strategy is subject to appropriate disciplinary action.

### 15. REVIEW OF THE EFFECTIVENESS OF THE FRAUD PREVENTION STRATEGY

The Department will conduct a review of the Fraud Prevention Plan annually to determine the effectiveness thereof. The HOD is ultimately accountable with the assistance of the Department's Risk management section and the Risk Management Committee.

#### 15.1 Updating the Fraud Policy and Fraud Prevention Strategy

A central part of any fraud and corruption control program should involve an ongoing review of fraud and corruption risk exposures. Progress with the implementation of the fraud prevention strategy will be monitored by the HOD. Management is required to roll-out the strategy within their sections and monitor the progress thereof through management meetings and other formal interaction.

Fraud and corruption risk assessments will also be conducted annually at the same time as the review of the fraud prevention strategy. At organisational level, the custodian of this strategy is the Head of Department. The Head of Department is responsible for the administration, revision and interpretation of this strategy. This strategy will be reviewed annually and appropriate changes applied should these be required.

#### 15.2 Creating Awareness and Education

It is the responsibility of all Senior Managers and Managers to ensure that all employees under their area of responsibility are made aware and trained on this policy.

The Department's Risk management section is responsible for communicating relevant sections of this policy to members of the public or other stakeholders of the Department.

This component of the Strategy comprises two approaches, namely **education and communication**. In this regard, the Department will develop an **annual awareness programme** which will guide and integrate awareness initiatives. The implementation of the awareness strategy will be incorporated in the performance management system of the Risk Manager/Ethics Officer for accountability.

##### 15.2.1 Education

The Department will ensure that regular presentations and formal trainings are carried out for employees as part of the **awareness strategy** to enhance their understanding of the manifestations of fraud, prevention and detection techniques and the components of the Strategy, in general. These presentations and training will include ongoing formal lectures to managers in all functional disciplines.

##### 15.2.2 Communication

Communication is crucial in creating awareness of the Strategy amongst employees and other stakeholders. As part of the **awareness strategy**, **communication** is intended to facilitate a culture where all stakeholders strive to make the Strategy a success and to sustain a positive and ethical behaviour within the Department. This will increase the prospect of fraud being reported and improve Department prevention and detection ability.





## 2024/25 FRAUD PREVENTION PLAN / STRATEGY

The Department will consider various means of communicating its fraud prevention initiatives, including the following:

- (a) Conducting workshops and creating awareness of the Strategy;
- (b) Developing a poster campaign aimed at all stakeholders to advertise the stance of Department to fraud and its expectations with regard to the ethics and integrity of all stakeholders;
- (c) Circulating/sharing appropriate sections of the Code to other stakeholders, e.g. consultants and contractors;
- (d) Capturing a position statement of the Department in relation to fraud in all departmental correspondence and publications;
- (e) Publicising "lessons learned" out of investigations into allegations of fraud amongst employees;
- (f) Circulating successes related to the Strategy and fraud modus operandi;
- (g) Including an anti-fraud statement in all bid documents as part of the conditions of the tender;
- (h) Placing notices or other communiqués related to the Strategy in toilets and other areas to which employees and the public have access;
- (i) Placing communiqués in government vehicles, e.g. relating to the abuse of vehicles;
- (j) Developing a fraud prevention suggestion box where all employees could make suggestions on how to prevent fraud and corruption and further improve the Strategy;
- (k) Using the newsletter to communicate issues relating to the prevention; and
- (l) Detection of fraud, including matters reported and action taken.

In addition to the awareness and communication strategies discussed above, the Department will ensure that the Strategy is communicated on an ongoing basis, both internally and externally.

### 15.3 Reporting

The HOD will on a regular basis provide feedback to all identified internal stakeholders who could include the Audit and Risk Committee, on the fraud risk management initiatives. Such report may include the following (depending on which stakeholder reporting to):

#### 15.3.1 Fraud Incidents

- Summary of number of incidents reported and Business Unit impacted
- Update on investigation status
- Reporting of fraud incidents including the modus operandi and a trend analysis of which modus operandi is on the increase
- Commentary on the root causes of the fraud incidents and whether the fraud has been internally or externally perpetrated
- Recommendations on mitigating controls that will be implemented in order to prevent similar fraud incidents from re-occurring
- Reporting on losses incurred by the Department. Such reporting to include the actual gross losses, near misses and potential losses in order for the MEC to understand the organizations full exposure to fraud.

#### 15.3.2 Ethics

- Details on any violations to the ethics policies and procedures by staff, service providers, clients or third parties
- Fraud risk management initiatives
- Updates on the proactive and reactive fraud prevention and detection initiatives implemented
- Details on any recommendations by Internal Audit were not implemented by line management and the impact this has on the Department's efforts to manage its fraud risks



- Update on the Department's Fraud Risk Register and any changes to the control environment in mitigating the identified fraud risks.

### 15.3.3 Schedule of Reporting Obligations in terms of PRECCA

Section 34 of PRECCA contains very strict prescripts in this regard:

*“Any person in a position of authority who knows or ought reasonably to have known or suspect that another person has committed: Corruption or the offences of theft, fraud extortion, forgery or uttering of a forged document, involving R100 000 or more must report such knowledge or suspicion or cause same to be reported to a police official.”*

In terms of PRECCA, fraud, theft, corruption, and forgery matters above the R100 000 threshold, must be reported to the SAPS.

A person in a position of authority, as defined in the Act, includes, *inter alia*:

- The Director-General or Head, or equivalent officer, of a National or Provincial Department
- Any public officer in the Senior Management Service of a public body
- Any person who has been appointed as chief executive officer, or an equivalent officer, of any agency, authority, board, commission, committee, corporation, council, department, entity, financial institution, foundation, fund, institute, service, or any other institution or organisation, whether it is established by legislation, contract or any other legal means.



**2024/25 FRAUD PREVENTION PLAN / STRATEGY**

**E: COMPLIANCE WITH THE PREVENTION STRATEGY**


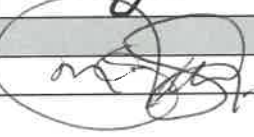
Any employee who fails to comply with the requirements of provisions of this Strategy is subject to appropriate disciplinary action.

**F: POLICY REVIEW**

This Strategy will be reviewed and updated every two years or as circumstances dictate.

**G: APPROVAL**

The Fraud Prevention Strategy is approved as follows:

DESIGNATION	NAME	SIGNATURE	DATE
<b>RECOMMENDATION</b>			
Risk Management Committee Chairperson	Mr. F. M. Mkhabela		27/03/2024
<b>Approval</b>			
Head Of Department	Mr. M.I. Kgantsi		28/08/24

