dcstm
Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

# DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT

## ANTI-CORRUPTION, ETHICS AND INTEGRITY STRATEGY

## 2025/2026

**TABLE OF CONTENTS** **PAGE**

## 1. GLOSSARY/ DEFINITIONS

| TERMS | DEFINITIONS |
|---|---|
| **Department** | North West Department of Community Safety and Transport Management. |
| **Ethics** | A broadly defined as well based standards of right and wrong that prescribe our rights, obligations and benefits to society. Ethics is about how we ought to live, treat others, run or manage our lives and organizations |
| **Risk Management** | A systematic and formalised process to identify, assess, manage and monitor risks. |
| **Risk** | An unwanted outcome, actual or potential, to the Institution's service delivery and other performance objectives, caused by the presence of risk factor(s).<br>Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such opportunities |
| **Risk Assessment** | Overall process of risk analysis and risk evaluation. |
| **Fraud** | The unlawful and intentional making of a misrepresentation which causes actual and or potential prejudice to another. The use of the term is in its widest possible meaning and is intended to include all aspects of economic crime and acts of dishonesty. |
| **Corruption** | 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 with the intention for personal gain. |
| **Employee** | a person who has been appointed permanently, notwithstanding that such appointment may be on probation, to a post contemplated in section 8(1)(a)of the Public Service Act, and includes a person contemplated in section(8)(b) or 8 (3)(c)of that Act who has been appointed on contract in terms of section 8(1) (c) (ii) of the Public Service Act. |
| **Departmental Management Committee (DMC)** | Refers to all executive and senior management of the Department, including any other official/s who are part of this Committee. |
| **Designated officials** | Employees determined by the Minister of Public Service |

| | |
|---|---|
| | Administration to declare their financial interest. |
| **NATIS** | National administration of traffic information system. |
| **PERSAL** | Personnel and salary system used in the Government. |
| **TRAFFMAN** | Traffic management system |
| **BAS** | Basic accounting system |
| **VMS** | Vehicle management system |
| **OLAS** | Operating licence administration system |
| **RAS** | Registration administration system |
| **AVS** | Abnormal Vehicle System |
| **PSR** | Public service regulations |
| **SSA** | State Security Agency |
| **SMS** | Senior Management Services |
| **ICT** | Information and Communication Technology |
| **VTS** | Vehicle Testing Station |
| **DLTC** | Driver, Learner Testing |

## 2. INTRODUCTION

Anti-corruption and ethics strategy is intended to meet requirements of the Public Finance Management Act (PFMA) and Treasury Regulations in dealing specifically with fraud risk. The strategy will continuously evolve as the Department makes changes and improvements in its drive to promote ethics, manage fraud and corruption risks and preventing it from materialising.

## 3. LEGAL MANDATE

a. **Sec 38(1)(a)(i) of the PFMA**, stipulates that the Accounting Officer / Authority is responsible for ensuring that the department, trading entity or constitutional institution has and maintains effective, efficient and transparent system of financial and risk management and internal control.

b. **Sections 3.2.1 and 27.2.1 of the Treasury Regulations** requires that risk assessment is conducted on regular basis and a risk management strategy, which includes a ***fraud prevention plan***, is used to direct internal audit effort. The strategy must be clearly communicated to all employees to ensure that risk management is incorporated into the language and culture of the department or entity.

c. **Public Service Regulations** 16c, 17(2), 18(3) of, 2016

## 4. FRAUD, CORRUPTION AND UNETHICAL BEHAVIOUR RISK GOVERNANCE

The Department of Community Safety and Transport Management has established a unit responsible to drive risk and integrity management. This unit is responsible amongst other activities to develop and implement policies to manage all types of risks including fraud, corruption and unethical behaviour. The Risk Management Committee and the Ethics Committee have been established to oversee risk and ethics processes within the Department.

## 5. PURPOSE AND OBJECTIVES

The purpose of the document is to provide guidance to all internal and external stakeholders of the Department on how it intends to prevent, detect and respond to the risk of fraud, corruption and unethical behaviour. The plan is developed to ensure compliance with the Provincial and National Anti-Corruption Strategies. Objectives of the plan are outlined as follows:

5.1 To provide Department's stance towards fraud, corruption and unethical behaviour

5.2 To provide basic understanding of what constitutes fraud, corruption and unethical behaviour

5.3 To clarify the roles and responsibilities towards fraud, corruption and unethical behaviour

This plan is developed to address all fraud and corruption risks which might occur including those identified during the departmental fraud risk assessment workshops.

## 6. COMMITMENT BY MANAGEMENT

The Departmental code of conduct and the fraud prevention plan/policy are not sufficient to prevent fraud and corruption; ethical behaviour needs to be embedded within the culture of the Department. Commitment from Executive and Senior Management and 'tone at the top' is key. Employees are more likely to do what they see their superiors doing than follow ethics policies, and it is essential that Management do not apply double standards. Management of this Department of Community Safety and Transport Management have expressed their commitment towards the fight against fraud and corruption by adopting policies and procedures relating thereto.

Fraud, corruption and unethical behaviour represent a significant potential risk to Department's assets, service delivery efficiency and reputation.

Management therefore commits to provide ethical leadership in order to inculcate and maintain ethical culture within the Department over time.

The Department also will not tolerate corrupt and/or fraudulent activities, whether internal or external and will vigorously pursue and prosecute any party, by all legal means available, which engage in such practices or attempt to do so. It also views attempted fraud as seriously as accomplished fraud.

The Department recognises the fact that possible acts of fraud and corruption by its employees and other stakeholders seriously deplete the scarce resources available in fulfilling its mandate, hence the Department support and adopt a culture of zero tolerance to fraud and corruption.

## 7. DEFINITION OF FRAUD AND CORRUPTION

**7.1** In South Africa fraud is commonly defined as the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another (CR Snyman). The term is also used in a wider sense to include all aspects of economic crimes and acts of dishonesty.

**7.2** The general offence of Corruption is contained in Section 3 of the Prevention and Combating of Corrupt Activities Act. Corruption refers to any conduct or behaviour where a person accepts, agrees or offers any gratification for him/her or for another person where the purpose is to act dishonestly or illegally with the intention for personal gain.

HK

Alternatively, corruption can be defined as, unlawful use of an official position to gain an advantage in contravention of one's duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail.

**7.3** Ethics is not a legally defined phenomenon, however the Department of Public Service and Administration defines ethics in broad terms as standards of right and wrong that prescribe rights, obligations and benefits to society. Ethical behaviour results when one does not merely consider what is good for oneself, but also what is good for others. Both the self and the other can refer to an individual, a group, or an organization.

**Table 1**

**Examples of Corrupt actions and schemes**

a. **Conflict of interest** – having interest in the transaction of the employer.
b. **Bribery & Kickbacks** – receiving arranged benefit(s) from the service provider.
c. **Illegal gratuity** – accepting gifts and/or benefits without required authorisation.
d. **Economic extortion** – persuading and/or threatening service providers to offer benefit(s).
e. **Abuse of authority** - when a public servant uses his/her vested authority to improperly benefit another person or entity.
f. **Favouritism** - provision of services or resources according to personal affiliations (ethnic, religious, party-political affiliation) of a public servant / person.
g. **Nepotism** - Showing unfair favour towards relatives, rather than applying an objective evaluation of the ability or suitability of the person or the public servant.
h. **Cronyism** - partiality to long-standing friends, especially by appointing them to positions of authority, regardless of their qualifications.

**Examples of Possible fraudulent activities identified during the risk assessment processes.**

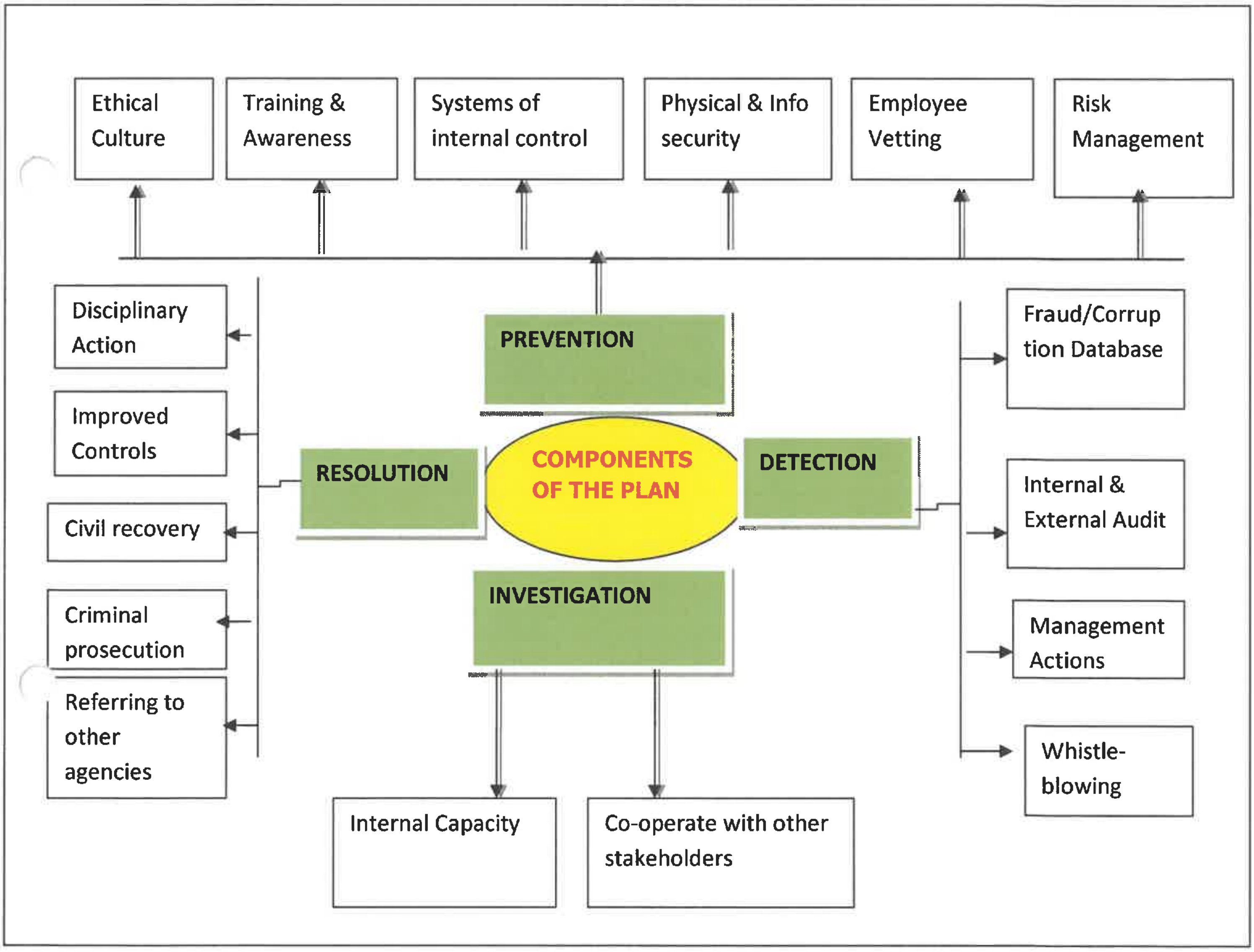
a. Unethical conduct by officials and service providers/clients of the Department
b. Insufficient monitoring of delivery of procured goods
c. Inadequate performance of Security service providers (security companies).
d. Issuing of driving/learners licences to unqualifying learners and drivers.
e. Loss of Departmental assets.
f. Acceptance of gifts and donations without following laid down procedures.
g. Traffic officials receiving bribery from motorist
h. Inadequate monitoring of implementation of overtime

HK

**Refer to Departmental fraud/corruption and misconduct register**

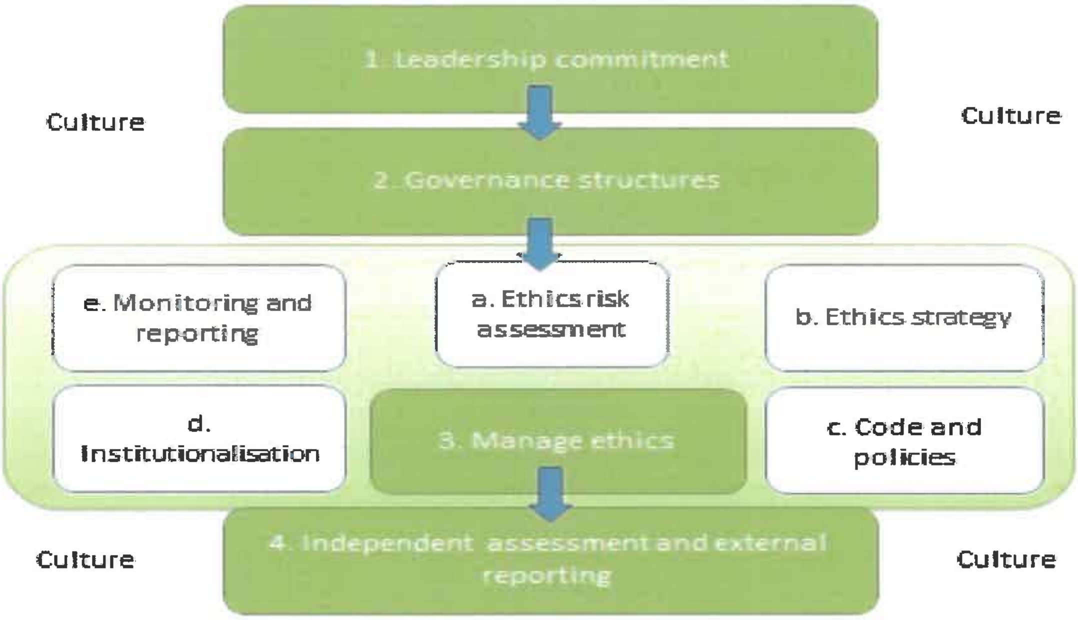
## 8. THE COMPONENTS OF THE PLAN

The main components of the plan, which may also be referred to as pillars of Anti -Corruption are represented in the schematic diagram as follows and will be discussed in detail below:



### *8.1 PREVENTION STRATEGIES*

#### 8.1.1 Ethical Culture / Code of conduct



a) The code of conduct for Public Service is applicable and acts as a guide to the Departmental employees as to what is expected from an ethical point of view, and therefore has been adopted as the ***code of ethics or conduct for the Department***.

b) The Department expects all its clients and stakeholders that are in any way associated with it to be honest and fair in their dealings. All employees are expected to lead by example in these matters.

c) The Department will pursue the following steps to communicate the principles contained in the code:

i.a copy of the code will be circulated to all employees for the future reference after the induction.

There are quite a number of guidelines in Public Service which strives to create and promote an ethical organisational culture and to which the Department fully support and subscribe to. Ethical conduct in the public service is required by the Constitution and it is the cornerstone of sound governance and a core responsibility of public office. The Department is therefore providing guidelines in terms of dealing with the following:

HK

### 8.1.2. Declaration of Business Interests

To promote ethical conduct and transparency, all employees must declare any business interests they hold, as well as those of their spouses, business associates, and/or close family members, that may result in a conflict of interest. The Department has developed specific declaration forms:

**Annexure A**: For employees to declare their business interests.
**Annexure B**: For employees to declare the business interests of their spouse, business associates, and/or close family members.

These declarations must be submitted annually or updated whenever there is a material change. Failure to disclose such interests may result in disciplinary action.

### 8.1.3. Officials conducting business with an Organ of State

The Department prohibits employees, in line with Regulation 13 (c) of the PSR, 2016, and Section 8 of the PAMA 2014, from conducting business with an organ of state *(directly or indirectly)* or be a director of a public or private company unless such an employee, is in an official capacity a director of a company listed in Schedules 2 and 3 of the Public Finance Management Act. These regulations contribute towards the enhancement of the value system which guides the professional conduct of employees in the public service.

The Department further prohibits its employee from registering on the National Treasury Central Supplier Database (CSD) as an individual, owner of a company or director of a public or private company unless such employee is in an official capacity is a director of a company listed in schedule 2 and 3 of the Public Finance Management Act. This is to align itself with the requirement of the Directive on Doing Business with an Organ of the State, published by the DPSA in February 2024.

The Department's Supply Chain Management policy must explicitly emphasis the requirement for Supply Chain officials to check the CSD before concluding any contract with suppliers and not allowing appointment of companies whose directors or members are employees appointed in the Public Service, either in their personal capacity or through a company or close corporation.

Failure to comply with the provision of the Regulation and Act will result in the following actions:

| Transgression | 1st Offence |
|---|---|
| **Conducting business with an Organ of State** | Serious Offence<br>Formal Disciplinary enquiry<br>Sanction: Dismissal<br>Fine or imprisonment for a for a period not exceeding 5 years or both such fine and imprisonment |

### ii. Other remuneration work outside the Department

Sec. 30 (1) of the PSA 1994 requires that employees must not perform or engage to perform other remunerative work outside the Department except with the written permission from the EA. Failure to comply with the provision of the Act will result in the following actions:

| Transgression | 1st Offence |
|---|---|
| **Failure to apply for permission to perform other remunerative work.** | Serious Offence which requires a disciplinary enquiry,<br>a) Invoking Sec 31 of the Act - Recovering the proceeds of other remunerative work<br>b) Sanction may include demotion as an alternative to dismissal OR dismissal |
| **Provision of false, inaccurate or incomplete information on the application form (to conceal conflict of interest)** | Serious Offence,<br>Formal Disciplinary enquiry<br>Sanctions that may be applied include:<br>a) Suspension without pay for a period not exceeding 3 months<br>b) Demotion as an alternative to Dismissal or,<br>Dismissal |

### ii. Financial disclosure

The risk to good governance arising from the conflict of interest does not face employees in senior management positions only. Decision making powers are often decentralised to lower level employees who may also face a conflict of interest situation in discharging their duties and

Hk

responsibilities. Disclosure of financial interest should, therefore, not be limited to employees in senior management positions but extended to other categories of employees who may be at risk of unethical behaviour arising from the conflict of interest situations and/or corruption.

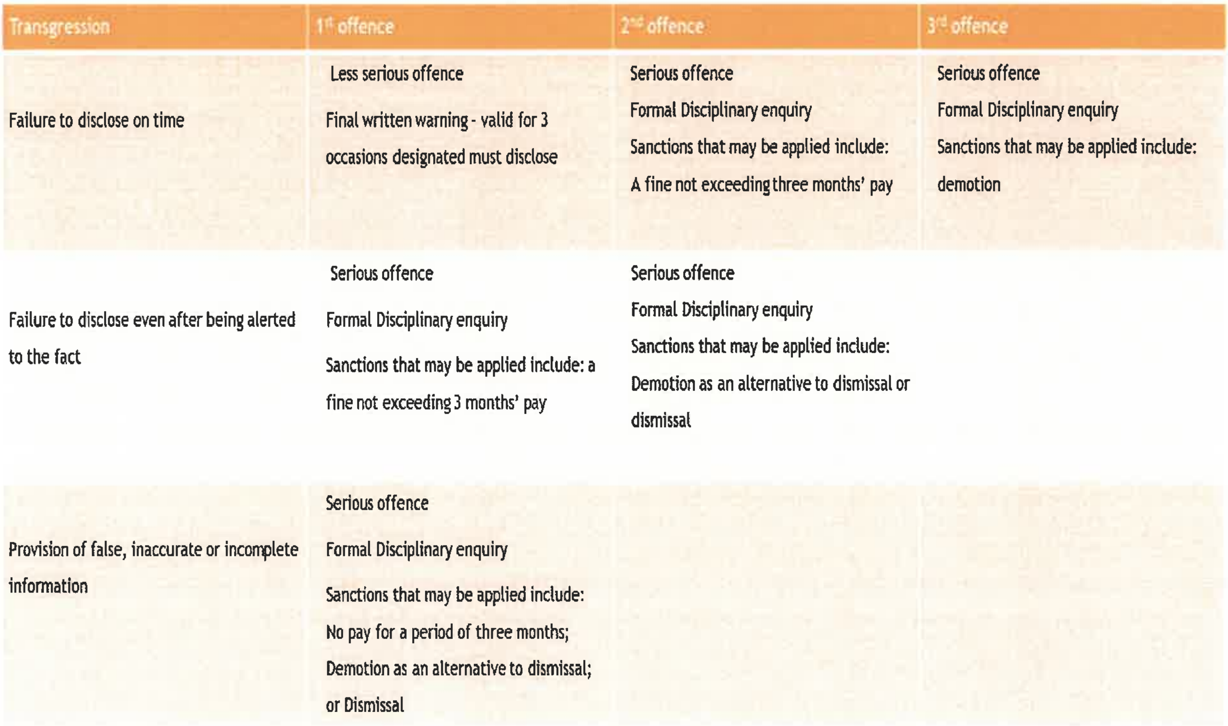
a) Financial disclosure for SMS members,

A financial disclosure framework was introduced in 2001 to assist executive authority to identify and manage conflict of interest among employees in senior management positions. The Department has processes in place to ensure compliance to the framework in relation to financial disclosure for SMS members.

b) Financial disclosure for designated members,

All employees at salary level 11 & 12, employees appointed at salary level 9 & 10 employees at supply chain management and financial management below level 9, ethics officers, employees earning equivalent of salary level 11 & 12 through OSD are also expected to disclose their financial interest on the eDisclosure system. Employees authorised (departmental admins) to reset the password of users who lock their accounts on the eDisclosure system shall also disclose their financial interest.

Failure to comply with disclosure requirements will results in disciplinary action being taken as follows:



| Transgression | 1st offence | 2nd offence | 3rd offence |
|---|---|---|---|
| Failure to disclose on time | Less serious offence<br>Final written warning - valid for 3 occasions designated must disclose | Serious offence<br>Formal Disciplinary enquiry<br>Sanctions that may be applied include:<br>A fine not exceeding three months' pay | Serious offence<br>Formal Disciplinary enquiry<br>Sanctions that may be applied include:<br>demotion |
| Failure to disclose even after being alerted to the fact | Serious offence<br>Formal Disciplinary enquiry<br>Sanctions that may be applied include: a fine not exceeding 3 months' pay | Serious offence<br>Formal Disciplinary enquiry<br>Sanctions that may be applied include:<br>Demotion as an alternative to dismissal or dismissal | |
| Provision of false, inaccurate or incomplete information | Serious offence<br>Formal Disciplinary enquiry<br>Sanctions that may be applied include:<br>No pay for a period of three months;<br>Demotion as an alternative to dismissal;<br>or Dismissal | | |

### 8.1.2 Training and awareness

The primary function of training new and existing employees on this plan is a fundamental process that inculcates the Department's culture and philosophy of zero tolerance on fraud and corruption to all employees.

Fraud is often highlighted through a tip off and therefore it is essential that all employees are made aware of:

i. What constitutes fraud?

ii. How to identify fraudulent behaviour, and

iii. How to respond if they suspect or detect instances of fraud or corruption.

Training and awareness is more likely to decrease rather than increase the number of fraudulent incidents.

In this endeavour, a special attention will be paid to high risk areas like procurement of goods and services, licensing inspectorate, road traffic management, abnormal loads, scholar transport, taxi operator permits and other permits, human resource management, revenue collection, etc.

Employees may be educated through a number of mediums, such as formal training sessions, group meetings, posters and pamphlets, newsletters, payroll bulletins or awareness pages on internal websites.

### 8.1.3 Systems of internal controls

A System of internal control is viewed as the most valuable fraud prevention device the Department can invest in. An internal control system comprises all those policies and procedures that taken together, support Department's effective and efficient operation. Internal controls typically deal with factors such as review, approval and authorisation processes, access restrictions and transaction controls, account reconciliations, and physical security.

In addition to internal control mechanisms, the **Department will integrate Ethical Assessments** as part of the control process to ensure ethical behaviour from the start of an employee's journey (as required by the directive on the HRDM for public service professionalization volume 1"). This will include:

- **Ethical Assessments in Recruitment:** Scenario-based interviews, ethical reasoning tests, and essays on ethical frameworks and codes of conduct, which will form part of the recruitment and selection process for all levels of appointments. These assessments are crucial to identifying potential risks before individuals are hired, reinforcing a culture of integrity from the

HK

outset. The Human Resource Management unit must ensure compliance to this requirement during the recruitment processes.

- **Ongoing Ethical Training and Monitoring:** Regular training on ethical conduct, awareness of fraud risks, and how to deal with unethical practices, ensuring that ethical behaviour is maintained throughout an employee's career

The Department's internal controls will be regularly reviewed to address new risks, such as emerging fraudulent methods, legislative changes, or evolving technologies, and will continually improve to reflect these changes.

The Department has quite a number of policies, procedures, and regulations designed to ensure compliance with government legislation and to limit risks, including the risks of fraud and corruption. These include, but are not limited to:

a. **Supply Chain Management policies**
   i. requires all Bid Committee members to disclose conflict of interest during their sittings,
   ii. requires completion of SBD forms by suppliers to disclose any interest they might have in the Department, etc.

b. **Human Resource policies**
   i. requires interview panel members to disclose their interest,
   ii. requires employees to sign a code of conduct declaration forms,

c. **Financial Management policies**
   i. which requires verification of payments to ensure authentication and detection of any fraudulent claims made by the suppliers or employees
   ii. Requires reconciliations and monitoring of bank transactions which will detect any unauthorised transactions.

Whenever new internal control procedures are introduced, they should be documented clearly and simply, in order that any deviation can be identified. Internal controls will be regularly reviewed as part of the risk management process, and there should be continual improvement of controls in light of new risks, such as new changes in operation due to changes in legislation or technologies, changes in structure, or innovative fraudsters. ***Existence of control systems is one issue and compliance to such controls is of utmost importance.***

HK

### 8.1.4 Physical and Information Security

**Physical Security**

Recognising that effective physical security is one of the "front line" defence mechanisms against fraud, the Department will take regular steps to improve physical security and access control at its offices in order to limit the risk of theft of assets and valuable records, such as computer equipment and bid documents.

Security sub directorate will conduct regular review in both Head Office and regional offices, weaknesses identified during these reviews will be addressed to ensure compliance with MISS policy.

**Information Security**

The Department has a number of IT applications in its operation (eNATIS, PERSAL, TRAFFMAN, BAS, VMS, OLAS, etc). Some of these systems have built in controls to guard against manipulation by users.

Security tips are also distributed on an ongoing basis to alert users of the security risks and measures to deal with such risks.

Department must ensure that employees leaving due to suspension, resignation, transfer or retiring are removed from e-mail and other systems with immediate effect.

### 8.1.5 Employee Vetting

Currently the Department is referring documents for all appointments made to SSA for verifications and vetting. All employees are issued with vetting forms which are then referred to SSA which an agent is appointed by government for this purpose.

**Pre-employment screening**

Pre-employment screening is the process of verifying the qualifications, suitability and experience of a potential candidate for employment. Techniques used include confirmation of educational and professional qualifications, verification of employment background and criminal history and credit checks.

Screening applicants should reduce the likelihood of people with a history of dishonest or fraudulent behaviour being employed within the Department, and is therefore an important fraud prevention procedure. The Department extends this exercise to candidates for promotions and transfers as well.

HK

### 8.1.6 Conducting Exit interviews

Conducting exit interview on terminated (transfers and retired) and/or resigning interviews may serve as preventative and detection measure of fraud. These interviews will assist Department to determine whether there are issues regarding management's integrity or information regarding conditions conducive to fraud. Review of the details on the resignation letter and information gathered during the interview will assist in checking whether opportunities for fraud exist in the Department. Human Resource Administration is charged with the responsibility to perform the function and report to management on the outcomes.

### 8.1.7 Returning of allocated resources

Resources allocated to employees to enable them to carry out their duties are instruments that can perpetrate fraud, corruption and unethical behaviour. The Department must therefore ensure that such resources are returned with immediate effect or within the notice period. ICT Resources such as laptops, hard-drives; uniform for traffic officials, fire-arms, two-way communication radio, blue lamps, etc. must be returned to the Department upon leaving due to resignation and/or retirement.

### 8.1.8 Risk Management

**Periodic assessment of corruption, ethics and integrity risks**

In order to manage fraud and corruption risks, the Department periodically identify the risks of corruption and ethics it may be exposed to so that appropriate mitigating strategies are put into place. Corruption and ethics risks are identified for all processes of the business and then assessed in terms of impact and likelihood.

In addition to the monetary impact, the assessment should consider non- financial factors such as reputation. An effective **corruption, ethics and integrity** risk assessment will highlight risks previously unidentified and strengthen the ability for timely prevention and detection of fraud. Opportunities for cost savings may also be identified as a result of conducting the fraud risk assessment.

Progress reports on reported cases / incidents of fraud and corruption occurring in the Department will be shared by the responsible manager (HRM) with the Risk and Integrity Management Unit for updating of the **corruption, ethics and integrity** risk register and further discussed in the Risk Management and Ethics and Integrity Committee meetings.

In the exercise of identifying fraud risks the Department also consider the risk of **management overriding controls and** populate the fraud risks from internal & external sources. Also consider fraud risks resulting from ICT systems used in operations, regulatory, misconduct and reputation risks.

Though the Department acknowledges that fraud, corruption and unethical behaviour may occur in all programmes and sub programmes; it commits to put more efforts and intensify controls in the following areas which are highly susceptible to the risk of fraud and corruption:

- Supply Chain Management processes
- Human Resource Management processes
- Financial Management systems
- Information Technology procedures
- Law Enforcement
- Issuing of learners and drivers licences
- Issuing of abnormal loads and operators permits
- Public Transport services (Learner and commuter transport)
- Government motor fleet

**FRAUD RISK RATING TABLES**

**Impact**

The following is a guide to be utilised to assess the potential impact of fraud risks.

| Rating | Assessment | Definition |
|---|---|---|
| 1 | Insignificant | There is 90-100% that controls will prevent fraud. **(Unacceptable- Action must be taken immediately)** |
| 2 | Minor | There are 70-89% chances that it is likely that the controls will prevent fraud. **(Unacceptable- Action must be taken)** |
| 3 | Moderate | There are 50-69% chances that it is likely that the controls will prevent fraud. **(Unacceptable- Action must be taken)** |
| 4 | Major | There are 30-49% chances that it is likely that the controls will prevent fraud. **(Unacceptable- Action must be taken)** |
| 5 | Critical | There are 1-29% chances that it is likely that the controls will prevent fraud. **(Unacceptable- Action must be taken)** |

## Likelihood

The following is a guide to be utilised to assess the likelihood of fraud risks.

| Rating | Assessment | Definition |
|---|---|---|
| 1 | Rare | Fraud is conceivable but is only likely to occur in extreme circumstances. |
| 2 | Unlikely | Fraud may occur infrequently and is unlikely to occur within the next 12 months |
| 3 | Moderate | There is an above average chance that fraud will occur at least once in the next 12 months |
| 4 | Likely | Fraud could easily occur, and is likely to occur at least once within the next 12 months |
| 5 | Common | Fraud is already occurring, or is likely to occur more than once within the next 12 months |

Inherent risk exposure (impact X likelihood): Residual risk exposure (inherent risk X control effectiveness)
The following is a rating table to be utilised to categorise the various levels of inherent and residual risk.

| Risk rating | Inherent 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) |

Impact and likelihood

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| LIKELIHOOD | 5 | Frequent | 5 | 10 | 15 | 20 | 25 |
| | 4 | Likely | 4 | 8 | 12 | 16 | 20 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 3 | Moderate | 3 | 6 | 9 | 12 | 15 |
| | 2 | Unlikely | 2 | 4 | 6 | 8 | 10 |
| | 1 | Rare | 1 | 2 | 3 | 4 | 5 |
| | | | Insignificant | Minor | Moderate | Major | Critical |
| | Rating | | 1 | 2 | 3 | 4 | 5 |
| | IMPACT | | | | | | |

## *8.2 DETECTION STRATEGY*

### 8.2.1 Internal and External Audit

The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the Department and Management. It is important that Management, with the oversight of those charged with governance, place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment.

The primary objective of Internal Auditors provides reasonable assurance that fraud controls are sufficient for identified fraud risk and that the controls are functioning effectively. However, in performing their engagements they should exercise professional scepticism when reviewing activities and be on the guard for the signs of fraud and corruption.

Both Internal and External auditors are also responsible to report any suspected acts of fraud or corruption detected during their audit process to Management.

### 8.2.2 Management Actions

Managers should exercise their responsibilities and accountability with due care as they perform their duties on reviews and approval of documents. This will enable them to identify and rectify incorrect and fraudulent attempts by their staff members or any other parties. It is therefore important that management must have a basic understanding of all policies and procedures of the Department and government as a whole. There are other techniques which can assist in identifying areas of fraud and corruption.

**Following is amongst others; techniques which Management should adopt in identifying anomalies.**

**a) Background reading**: it is important to keep up to date with fraud trends and issues. The general press can be a useful source of information for this, along with technical magazines, which often carry articles on fraud and financial irregularity. Also useful is a subscription to a publication specialising in fraud or buying a good reference book. The Department provide access to Internet which is also a valuable, and vast, research tool.

**b) Risk assessment**: undertake a fraud risk assessment and design specific tests to detect the significant potential frauds identified through the risk assessment. Act on irregularities which raise concerns.

**c) Benchmarking**: comparisons of one financial period with another; or the performance of one cost centre, or business unit, with another; or of overall business performance with industry standards, can all highlight anomalies worthy of further investigation.

**d) Ratio analysis**: can be used to identify any abnormal trends or patterns.

**e) Exception reporting**: many systems can generate automatic reports for results that fall outside of predetermined threshold values (exceptions), enabling immediate identification of results deviating from the norm.

### 8.2.3 Whistle blowing and reporting mechanism (National Anti-Corruption Hotline 0800 701 701)

Effective reporting mechanism is one of the key elements of a fraud prevention programme and can have a positive impact on fraud detection. The Department has therefore developed a whistle blowing policy which is intended to guide employees in reporting fraudulent activities and malpractices or maladministration realized in the Department. It also recognizes that whistle blowers may be victimized in contravention to the Protected Disclosures Act. This could have severe negative implications for the Department, e.g. negative media publicity.

### 8.2.4 Benefits derived from whistle blowing:

a. Deter wrongdoing,
b. Pick up potential problems early,
c. Enable critical information to get to the people who need to know and can address the issue,
a. Reduce the risk of anonymous and malicious leaks,
b. Minimise costs and compensation from accidents, investigations, litigations and regulatory inspections,

c. Maintain and enhance reputation of the Department.

### 8.2.5. Suggestion Boxes /Complaints boxes.

The Department has a suggestion/complaints box system implemented across programmes at Head Office and in the Districts through HRM. The primary objective of this initiative is to address service delivery shortcomings by promoting internal communication, employee involvement, and operational efficiency. Additionally, management will evaluate submitted suggestions and complaints to identify and address any incidents, including fraud and corruption-related concerns.

### 8.2.6. Fraud, Corruption and unethical behaviour database

The Department has a fraud and corruption database in place to record all reported cases. This database is used to monitor the progress of investigations and will be considered when conducting fraud risk assessments.

## *8.3 INVESTIGATION AS A STRATEGY*

Any fraud and corruption committed by an employee or any other person against the Department will be pursuit by thorough investigations and to the full extent of the law. Investigation will be conducted internally or referred to external bodies, depending on the nature of the transgression to be investigated.

Preliminary Investigation will be conducted internally to establish as to whether there is a case, and thereafter full investigation will be conducted. As to who will be conducting the investigation will depend on the type of case.

## *8.4 RESOLUTION OF FRAUD AND CORRUPTION*

### 8.4.1 Disciplinary code and procedures

a) The disciplinary code and procedures of the Department prescribes appropriate steps to be taken to resolve disciplinary matters.

b) The Department recognises the fact that consistent and effective application of a disciplinary measure is an integral component in making this plans a success. It will continue to pursue the following steps to ensure a consistent, efficient and speedy application of the disciplinary measures:

I. Ensuring that all managers are aware of the content of the disciplinary code and procedures, standards of discipline expected, the procedure for application of the disciplinary measures and the disciplinary process; and;

tk

II. Ensuring the consistent application of disciplinary measures through the existing monitoring system, which includes proper record-keeping of all disciplinary actions taken

c) Where employee of the Department is found guilty of acts of fraud and corruption, the following actions will be taken against him/her:

I. Taking a disciplinary action within a reasonable period of time after the incidents.

II. Discipline will be applied in a consistent, unbiased and fair manner irrespective of the official's position in the organisational structure to ensure that fraud and corruption are dealt with effectively;

III. Instituting recovery of financial losses, including formal civil action;

IV. Initiating criminal prosecution by reporting the matter to SAPS, HAWKS, Assets Forfeiture Unit, or any other relevant law enforcement agency; and any other appropriate and legal remedy available.

d) Where service providers and other stakeholders are found guilty of acts of fraud and corruption, the following actions will be considered against him or her:

I. Report the matter to SAPS, HAWKS, or any other relevant law enforcement agency.

II. Prohibit the supplier from doing business with the Department in future by reporting the client or supplier to the National Treasury for blacklisting; and

III. Any other appropriate and legal remedy available.

### 8.4.2 Improved internal controls

Prevention, detection, corrective, directive controls and segregation of compatible functions are basic internal controls designed to prevent and detect fraud and corruption also to ensure that systems are properly implemented. These are embedded in the policies, procedures, IT operating systems, regulations and other Departmental prescripts and are effectively implemented as fraud risk deterrent strategies.

## 9. FURTHER IMPLEMENTATION AND MONITORING

### 9.1 Creating awareness

This component of the plan comprises of two approaches, namely education and communication.

#### a) Education

The Department will ensure that regular presentation and formal training are carried out for employees to enhance their understanding of manifestation of fraud prevention and detection techniques, and the components of the plan. These presentation and training will include ongoing formal lectures for

HF

supervisors and managers in all functional discipline, with particular emphasis on Human Resources, Supply Chain Management and Financial Management

**b) Communication**

The objective of the communication strategy is to create awareness of the plan amongst employees and other stakeholders. This is intended to inculcate a culture where all stakeholders strive to contribute towards making the Plan successful as well as for the sustaining of a positive culture within the Department. This will increase the prospect of fraud being reported, improve the Department's prevention and detection ability and address negative perceptions about the Department.

## 10. ONGOING MAINTANANCE AND REVIEW

### 10.1 Ethics and Integrity Management Committee

In order to ensure that the processes of ongoing development and implementation of the Plan is consultative, and viewed as such by all stakeholders within the Department, Ethics and Integrity Management Committee has been appointed which also deals with issues relating to fraud and corruption. The Committee is responsible for providing oversight over the development of fraud and corruption prevention strategies. The role of the Ethics and Integrity Management Committee is spelled out in Ethics and Integrity Management Committee Charter.

**10.1.2** The plan will be reviewed at least once annually, whilst progress with the implementation of various components will be reported on a quarterly basis. In the latter regard, specific priorities stemming from the plan, actions to be taken, responsible person and feedback dates relating progress made will also be set.

## 11. FRAUD RESPONSE PLAN

**11.1** All cases received from internal processes or Office of the Premier through the Provincial or National Anti-Corruption Hotline (NACH) will be investigated by Human Resource Management and addressed as per Departmental policy.

**11.2** Cases identified during the inspections involving the external Registering Authorities (RAs) will be investigated in the same manner as internal cases, the South African Police Services (SAPS) and other law enforcement agencies will be involved depending on the nature of the case and recommendations of the Executive Authority.

**11.3** Mitigating strategies will also be developed to address identified fraud and corruption risks and implementation thereof will be monitored by the Risk & Integrity Management Directorate.

## 12. REVIEW OF THE POLICY

This policy shall be reviewed annually or as and when it is deemed necessary to reflect any changes that may occur in the Department.

## 13. EFFECTIVE DATE OF THE POLICY

This policy shall be effective from the date of approval by the Head of Department.

## 14. RECOMMENDATION AND APPROVAL

| DISCUSSED AND ADOPTED DURING | MEETING HELD DATE |
|---|---|
| EXECUTIVE MANAGEMENT COMMITTEE | 24/03/2025 |
| RISK MANAGEMENT COMMITTEE | 26/03/2025 |

**RECOMMENDED**

**MS VT LETEANE**
**CHAIRPERSON**
**DATE:** 28|03|25

**APPROVED**

**DR HANS KEKANA**
**HEAD OF DEPARTMENT**
**DATE:** 31|03|2025