

ANTI-FRAUD AND CORRUPTION POLICY 2025/2026



public works & roads

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

TABLE OF CONTENTS

1. BACKGROUND	3
2. PURPOSE.....	4
3. LEGISLATIVE BACKGROUND	4
4. DEFINITION OF FRAUD.....	5
5. SCOPE OF THE POLICY.....	6
6. APPLICATION OF PREVENTION CONTROLS AND DETECTION MECHANISMS	6
7. REPORTING PROCEDURES AND RESOLUTION OF REPORTED INCIDENTS	6
8. ROLE PLAYERS.....	8
9. PROSECUTION	10
10. IMPLICATIONS OF NON-COMPLIANCE WITH THE POLICY	10
11. POLICY REVIEW	11
12. POLICY MAINTENANCE	11



1. BACKGROUND

The Department of Public Works and Roads (DPWR) is fully committed to the fight against fraud and corruption, and will uphold the Batho Pele principles in all its dealings with the public, organizations, and third parties conducting business with the Department. The Department is dedicated to preventing, detecting, responding to, and discouraging any form of fraud or corruption.

The Member of the Executive Committee (MEC), Executive and Senior Management, as well as all staff within the Department, are expected to maintain the highest standards of ethical conduct and professional work ethic. Both the MEC and the Accounting Officer of the Department must ensure strict adherence to all ethical codes and standards. The Department expects all individuals, organizations, and third parties associated with or doing business with it to act with integrity, transparency, and a commitment to avoiding fraud and corruption.

Fraud and corruption severely undermine the government's ability to fulfill its constitutional mandate, which in turn erodes public trust and investor confidence. As one of the world's most progressive constitutions, South Africa has a robust legislative framework designed to protect citizens' rights, foster a fair and secure environment, and promote good governance. These mechanisms are vital to ensuring that public resources are used effectively and that all individuals have access to services in a just and accountable manner.

The National Government has introduced the "Batho Pele" initiative, which aims to transform public service delivery at all levels of government. This initiative is anchored in 11 key principles, namely:

- **Consultation**
- **Service standards**
- **Access**
- **Courtesy**
- **Information**
- **Openness and transparency**
- **Redress**
- **Value for money**
- **Encouraging innovation and rewarding excellence**
- **Customer impact**
- **Leadership and strategic direction**

The persistent issue of fraud directly contradicts and undermines the principles outlined in Batho Pele, particularly in areas such as transparency, accountability, and service delivery. Combating fraud is not only about upholding the law but also about fostering a culture of integrity and respect within the public service. The Department remains resolute in its commitment to these principles and will continue to prioritize the eradication of fraud and corruption at every level of operation.



2. PURPOSE

- 2.1 This policy outlines the stance of the Department of Public Works and Roads (DPWR) on "fraud," as defined in paragraph 2.2 below. It aims to reinforce and complement existing systems, policies, procedures, rules, and regulations designed to deter, prevent, detect, respond to, and mitigate the impact of fraud. The Fraud Response Plan, which complements this Policy, details the DPWR's approach to responding to allegations of fraud.
- 2.2 The purpose of this document is to affirm DPWR's commitment to fostering a culture of zero tolerance towards fraud in all its forms. DPWR strives to uphold the highest ethical standards and maintain transparency and accountability in all operations.
- 2.3 DPWR acknowledges that fraudulent activities by its employees severely undermine the limited resources available to fulfill its mandate and objectives. These acts compromise the organization's ability to deliver essential services to the public.
- 2.4 In addition to the direct financial losses, DPWR recognizes that the broader consequences of fraud can have far-reaching effects, damaging not only financial assets but also the organization's ability to achieve its mission.
- 2.5 Although difficult to quantify, acts of fraud—if left unchecked—can have a significant and detrimental impact on:
 - The quality and effectiveness of service delivery;
 - The strength of business relationships with clients, suppliers, and the public;
 - Employee morale and productivity;
 - The reputation and public image of DPWR.

3. LEGISLATIVE BACKGROUND

The following legislation provides the legal framework for addressing fraud and related activities within the Department of Public Works and Roads (DPWR):

- **Prevention and Combating of Corrupt Activities Act, 2004:** Establishes measures to prevent and combat corruption, including the criminalization of corrupt activities in both the public and private sectors.
- **Public Finance Management Act, 1999:** Regulates the management of public finances, ensuring transparency, accountability, and effective use of state resources.
- **Public Service Act, 1994:** Governs the administration of the public service, outlining the responsibilities of public servants and setting standards for ethical conduct.
- **Protected Disclosures Act, 2000:** Protects whistleblowers by providing mechanisms for the reporting of unethical behavior, including fraud, without fear of retaliation.



- **Promotion of Access to Information Act, 2000:** Promotes transparency and accountability by ensuring that information held by public bodies is accessible to the public.
- **Financial Intelligence Centre Act, 2001:** Establishes the Financial Intelligence Centre to collect, analyze, and disseminate financial intelligence to combat money laundering and other financial crimes.
- **Prevention of Organized Crime Act, 1998:** Addresses activities related to organized crime, including provisions for the forfeiture of criminal assets and the prevention of financial crimes.

4. DEFINITION OF FRAUD

- 4.1 Fraud is a term that is interpreted in various ways in South Africa, often encompassing corruption, especially in the public domain. In many contexts, the definition of fraud is extended to include acts of corruption, given their overlapping nature.
- 4.2 For the purposes of this policy, fraud is defined in line with a well-established and authoritative definition provided by South African criminal law jurist C.R. Snyman, who describes fraud as: “The unlawful and intentional making of a misrepresentation that causes actual prejudice or has the potential to prejudice another.”
- 4.3 Fraudulent activities, as defined in this policy, include, but are not limited to, the following actions:
- Any dishonest, fraudulent, or corrupt act;
 - Theft of funds, supplies, or other assets;
 - Maladministration or financial misconduct in the handling or reporting of money, financial transactions, or other assets;
 - Making a profit from insider knowledge or confidential information;
 - Disclosing confidential or proprietary information to external parties for financial or other personal advantage;
 - Requesting or accepting anything of material value (free of charge) from contractors, suppliers, or other persons providing goods or services to DPWR;
 - Irregular destruction, removal, or abuse of records, documents, or equipment;
 - Deliberately omitting or refusing to report, or taking no action upon reports of, irregular or dishonest conduct;
 - Bribery, blackmail, secret commissions, or extortion involving a DPWR employee in the performance of their duties;
 - Abuse of DPWR facilities for personal gain or improper purposes; and
 - Any similar or related fraudulent activity or irregularity.



5. SCOPE OF THE POLICY

This policy applies to all individuals and entities with whom the Department of Public Works and Roads (DPWR) interacts. All stakeholders are expected to uphold the principles outlined in this policy. Specifically, the policy applies to:

- **Public servants:** All employees and officials of DPWR, including management and staff.
- **Suppliers, contractors, and providers of goods and services:** Any external organizations or individuals engaged in business or contractual relationships with DPWR.
- **Users of services/customers:** Individuals or groups that utilize the services provided by DPWR.
- **Stakeholders, labor, and social organizations:** Any organizations, unions, or groups with a vested interest in DPWR's operations or activities.
- **Media and religious organizations:** Entities and individuals who engage with DPWR through reporting, coverage, or other forms of communication.

All other persons with links to the Department: Any other individuals or entities that have a formal or informal relationship with DPWR.

6. APPLICATION OF PREVENTION CONTROLS AND DETECTION MECHANISMS

In the event of any reported incidents of fraud, managers are required to promptly review the effectiveness of the controls that were compromised. Where necessary, managers should implement improvements to strengthen these controls and prevent similar irregularities from occurring in the future. This proactive approach ensures that the organization continually enhances its ability to detect, prevent, and respond to fraudulent activities.

7. REPORTING PROCEDURES AND RESOLUTION OF REPORTED INCIDENTS

7.1 What should employees do if they suspect fraud?

It is the responsibility of all employees to immediately report any suspected fraud or fraudulent incidents. Employees should report such allegations to their immediate manager. If an employee believes that their immediate manager is involved in the fraud, the report should be made to the next level of management.

All managers are required to report any incidents or allegations of fraud to the Head of Department.

Upon receiving the report, the Head of Department will notify the Risk Management Unit within the Department and/or the Forensic Services unit, which operates as a shared service under the Office of the Premier to initiate an investigation into the matter to assess and resolve the issue.



7.2 What should a member of the public do if they suspect fraud impacting DPWR?

If a member of the public suspects fraud affecting the Department of Public Works and Roads (DPWR), they are encouraged to report the matter. The public can contact any member of DPWR management, or they can report the allegation anonymously through the Fraud Hotline at the toll-free number **0800 701 701** or the Presidential Hotline at **17737**.

DPWR also encourages members of the public to reach out directly to the Head of Department, the Security Management Services Unit within DPWR, or the Forensic Services unit based at the Office of the Premier. Additionally, the Fraud Hotline contact details listed above are available for reporting fraudulent activities.

7.3 How will allegations of fraud be dealt with by DPWR?

7.3.1 The action taken by the Department in response to fraud allegations, whether raised by employees or members of the public, will depend on the nature of the concern. The matter may be referred to one or more of the following:

- The **Security Management Services Unit** within DPWR;
- **Forensic Services** based at the Office of the Premier;
- The **South African Police Service (SAPS)** or any other relevant law enforcement agency.

7.3.2 Supervisors and management within DPWR have access to advisory and supporting assistance from various units, including:

- **Risk Management Unit** within DPWR;
- **Security Management Services Unit** within DPWR;
- **Internal Audit Unit** within Provincial Treasury;
- **Human Resources Management**;
- **Forensic Services**, Office of the Premier;
- **Legal Services**;
- **Labour Relations**;
- The **Office of the Auditor-General**; and
- The **Public Protector**.

7.3.3 The **Risk Management Unit** and **Security Management Services Unit** collaborate to provide a more integrated strategic intelligence approach to:

- Support policy development and coordination of anti-fraud and corruption policies;



- Coordinate efforts among law enforcement agencies involved in combating fraud within the Province, including DPWR.

7.3.4 Supervisors and management within DPWR are supported by the full range of advisory and supporting units listed above.

7.3.5 Any fraud committed by an employee of DPWR will be thoroughly investigated and pursued to the full extent of the law. This includes consideration of the following actions:

- Taking **disciplinary action** within a reasonable timeframe after the incident;
- **Recovering financial losses**, including through formal civil action;
- **Initiating criminal prosecution** by reporting the matter to SAPS or another relevant law enforcement agency; and
- Pursuing any other **appropriate legal remedies** available.

7.3.6 The Head of Department and relevant managers are required to ensure that any losses or damages incurred by DPWR due to fraud committed by an employee or any other person are recovered from the individual found to be liable.

7.3.7 Upon receiving a fraud report from an external individual, the Head of Department or their delegated representative will:

- Acknowledge receipt of the concern;
- Inform the reporting individual (unless the report was made anonymously) about whether further investigations will be conducted, and if not, provide reasons for this decision.

7.3.8 DPWR recognizes the importance of ensuring that individuals, including employees, who report fraud are assured that their concerns have been properly addressed. Subject to legal constraints, information regarding the outcomes of investigations will be shared on a “**need-to-know**” basis.

7.3.9 The **Risk Management Committee** will regularly review reported fraud matters and the actions taken in response.

8. ROLE PLAYERS

8.1. Responsibility for Internal Controls

Management within the Department of Public Works and Roads (DPWR) is responsible for establishing and maintaining a sound system of internal controls that supports the achievement of departmental policies, aims, and objectives. The internal control system is designed to address and manage the full range of risks faced



by the department, with the management of fraud risk being an integral part of this broader risk management framework.

8.2 Overall Responsibility for Managing Fraud Risk

The overall responsibility for managing the risk of fraud has been delegated to line managers, the Security Management Services Unit, and the Risk Manager (Chief Risk Officer - CRO). The responsibilities of the Risk Manager (CRO) and Security Manager include:

- Developing a fraud risk profile and conducting regular reviews of fraud risks associated with key organizational objectives to keep the profile up-to-date;
- Designing and maintaining an effective control environment to prevent fraud from occurring;
- Establishing mechanisms for reporting fraud risks and significant incidents of fraud, and ensuring these are reported to the Chief Financial Officer (CFO) and Human Resources;
- Ensuring that all staff are aware of the department's stance on fraud and their individual responsibilities in combating it;
- Ensuring that appropriate anti-fraud training and development opportunities are provided to relevant staff;
- Ensuring that thorough and prompt investigations are carried out if fraud is suspected or detected;
- Taking appropriate actions to safeguard the recovery of assets;
- Ensuring that measures are taken to reduce the likelihood of similar frauds occurring in the future.

8.3 Responsibilities of Line Managers

Line managers are responsible for:

- Ensuring that an adequate system of internal controls is in place within their areas of responsibility, and that controls operate effectively;
- Preventing and detecting fraud within their areas;
- Assessing the risks involved in their operations and identifying fraud risks;
- Regularly reviewing and testing the control systems to ensure they are effective and compliant;
- Implementing corrective actions and new controls to prevent future fraud where incidents have occurred.

8.4 Responsibilities of Provincial Internal Audit Services

The **Provincial Internal Audit Services** is responsible for:

- Providing an opinion to management and the Audit Committee on the adequacy of arrangements for managing fraud risk, and ensuring that the department fosters an anti-fraud culture;
- Assisting in the deterrence and prevention of fraud by evaluating the effectiveness of controls, relative to the potential fraud risks across various operations of the department.



8.5 Responsibilities of All Staff

Every member of staff is responsible for:

- Acting with integrity in the use of departmental resources, and handling and managing departmental funds, whether related to cash, payment systems, receipts, or dealings with suppliers and customers;
- Being vigilant and recognizing that unusual events or transactions may indicate fraudulent activity;
- Immediately reporting any suspicion of fraud or unusual activities through the appropriate channels;
- Fully cooperating with internal checks, reviews, or investigations into suspected fraud.

9. PROSECUTION

9.1 Action Following Investigation

Where sufficient evidence is available following an investigation into the allegations, appropriate action will be taken against the implicated persons in accordance with the law.

9.2 Potential Actions

Appropriate actions may include, but are not limited to:

- **Disciplinary action** in line with DPWR's internal policies;
- **Referral to the South African Police Service (SAPS)** if evidence suggests that a criminal offence has been committed;
- **Civil recovery** of losses if evidence indicates that DPWR suffered financial loss due to the conduct of the implicated individual(s).

10. IMPLICATIONS OF NON-COMPLIANCE WITH THE POLICY

Officials who contravene any provisions of this policy will be subject to disciplinary proceedings, in accordance with:

- The **Disciplinary Code and Procedures** outlined in GPSSBC Collective Agreement No. 2 of 1999 for salary levels 12 and below;
- The **Senior Management Service (SMS) Handbook, Chapter 7**, for SMS members.



- Ethics Management Policy
- Financial Disclosure Policy

While this strategy strengthens the Department's ability to address fraud and corruption, it does not guarantee that such incidents will be fully prevented. Instead, it serves as a proactive tool to mitigate risks, promote ethical behaviour, raise awareness, and equip the Department to effectively handle instances of fraud and corruption.

The Department is committed to regularly reviewing and updating this strategy, ensuring its continued relevance and effectiveness in safeguarding public resources and upholding the highest standards of integrity.

7. THE OBJECTIVES OF THE STRATEGY

This plan outlines the Department's firm stance on fraud and corruption, reinforcing existing systems, policies, procedures, rules, and regulations aimed at preventing, detecting, responding to, and minimizing the impact of such dishonest activities. The strategy's primary objectives are to cultivate a culture of ethical conduct within the Department and to prevent, deter, detect, and address fraud and corruption effectively.

The objectives of the Strategy are to:

- **Promote Ethical Culture:** Establish a Departmental culture that is intolerant of unethical conduct, fraud, and corruption, fostering a commitment to ethical public service.
- **Prevent and Detect Fraud:** Implement proactive measures to prevent and detect unethical conduct, fraud, and corruption, minimizing vulnerabilities.
- **Investigate Irregularities:** Ensure all instances of unethical conduct, fraud, and corruption are thoroughly investigated, with the necessary actions taken.
- **Enforce Accountability:** Take appropriate action in response to detected irregularities, including disciplinary measures, recovery of losses, and, where necessary, prosecution.
- **Sanction and Redress:** Apply sanctions where applicable, including financial redress, to ensure consequences for fraudulent activities.
- **Enhance Administrative Efficiency:** Improve accountability, efficiency, and effective administration within the Department through robust controls and processes.
- **Encourage Participation:** Foster a collaborative approach, encouraging employees and stakeholders to actively contribute to the prevention and detection of fraud and corruption.
- **Promote Whistleblowing:** Ensure a safe environment where all officials, stakeholders, and the public feel encouraged and protected when reporting suspicious fraudulent activities without fear of reprisals.

The Strategy emphasizes that combating fraud and corruption is a shared responsibility across all levels of the Department and its stakeholders, strengthening the Department's commitment to maintaining a high standard of integrity and transparency.

8. COMPONENTS OF THE STRATEGY

The Fraud Prevention Strategy is designed to foster an environment where integrity is valued and unethical behaviour, including fraud and corruption, is actively discouraged. The goal is to create a culture of transparency and accountability within the Department. Below is a simplified look at how we approach preventing, detecting, and responding to fraud.



Fraud Prevention Strategy

Prevention

The first line of defense against fraud is creating an environment where unethical behaviour is simply not tolerated. This means setting clear expectations, providing training, and establishing policies that guide how we work.

Key prevention measures include:

- Code of Conduct for Public Servants (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 (e.g., Ethics Officer, Ethics Committees)
- Fraud Risk Assessments
- Recruitment Process – Employee Screening and Vetting
- Obligatory Leave Periods for employees in sensitive positions
- Probationary Periods for new employees
- Exit Procedures and Return of Assets to ensure proper handover
- Remunerative Work Outside the Public Service Policy
- Prohibition of Corrupt Individuals from Public Service
- Naming and Shaming of Corrupt Public Servants as a deterrent
- Vendor Due Diligence to ensure suppliers are vetted and monitored
- Review of Supply Chain Management – ensuring proper conduct by SCM officials in all government institutions
- Proper Delegation and Segregation of Roles within the SCM environment
- Blacklisting of Corrupt Suppliers
- Conflict of Interest Disclosures and Financial Disclosures
- Gifts and Donations Policy to regulate gifts and hospitality received
- Internal Controls to safeguard assets and mitigate risks
- Physical and Information Security measures to protect sensitive data and assets
- Security Screening of service providers
- Vetting of Staff to assess suitability for sensitive roles

Detection

Detection involves identifying existing instances of fraud and unethical conduct within the Department. The goal is to detect fraud as early as possible through active monitoring, reporting systems, and audits.

The goal is to detect fraud as early as possible through active monitoring, reporting systems, and audits.

Key detection measures include:

- **Vigilance by Officials** to report suspicious activities
- **Internal Audit Function** to regularly assess controls and detect irregularities
- **Whistle-blower Facility** to encourage anonymous reporting of suspected fraud

Response and Resolution

If fraud does occur, we must respond quickly and appropriately. This means taking swift action to limit the damage, investigating fully, and ensuring the right

- **Fraud Response Strategy:** We have a clear plan in place for how to deal with fraud when it's detected.
- **Cooperation with Anti-Corruption Agencies:** We don't work in isolation—if necessary, we partner with other organisations to investigate fraud thoroughly.

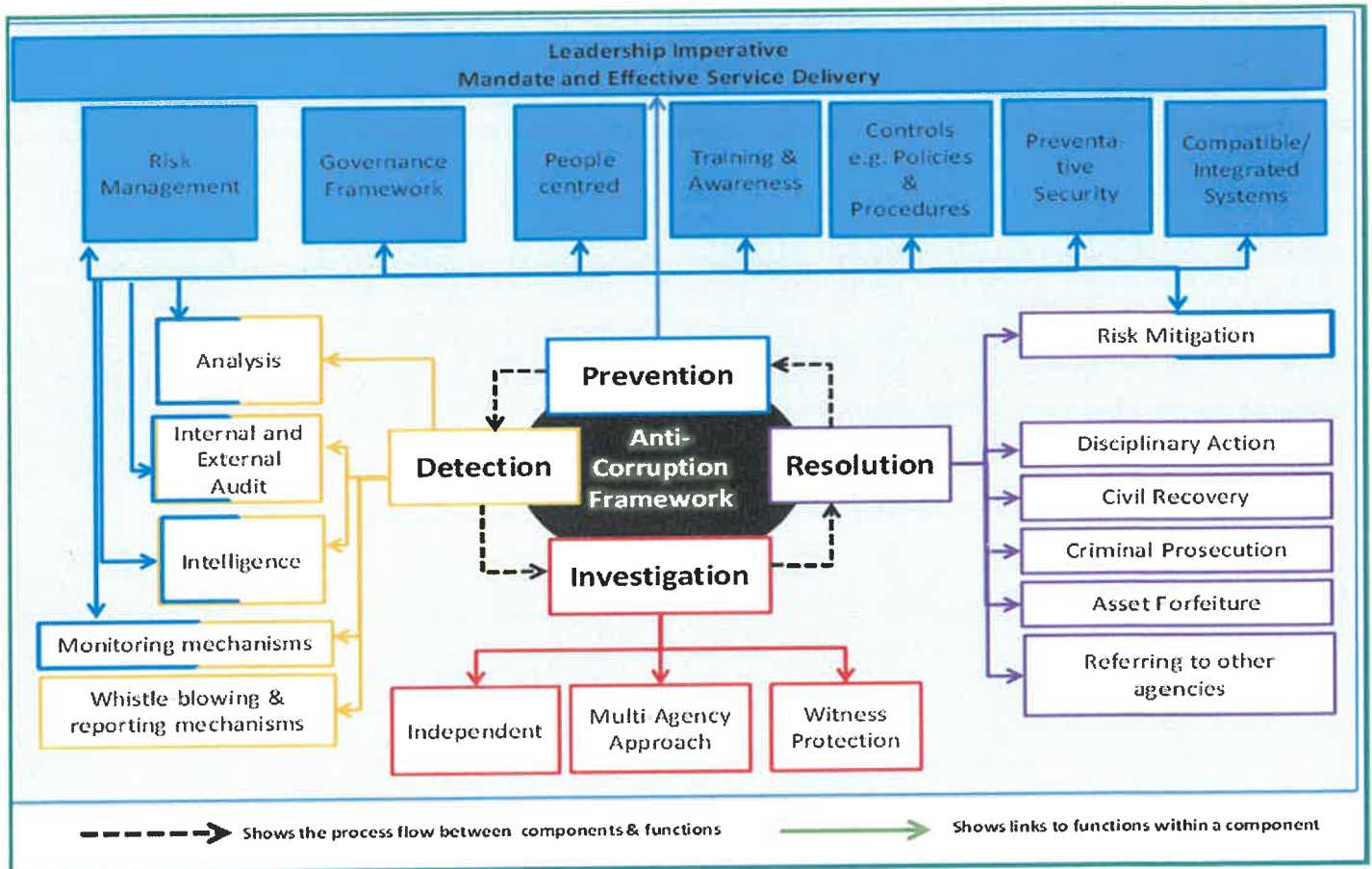


Fraud Prevention Strategy

measures are in place to hold wrongdoers accountable.

- **Disciplinary Action:** Employees found guilty of fraud face disciplinary procedures, in line with our policies.
- **Criminal Prosecution and Civil Recovery:** In serious cases, we will pursue criminal charges and work to recover any financial losses.

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



B: CREATING AN ETHICAL CULTURE

9. CREATING AN ETHICAL CULTURE

To reduce the motivation for and rationalization of fraud and corruption, the Department is committed to fostering an ethical culture and providing guidance to its employees regarding ethical conduct. Ethical conduct involves distinguishing between what is morally right and wrong, with the aim of doing what is right.

Our employees are expected to fulfill their obligations and conduct themselves according to the highest ethical standards, which encompass values such as integrity and honesty. The failure to uphold these

standards often leads to allegations of corruption and maladministration. The values and principles adopted by the Department are also reflected in Section 195 of the Constitution.

Section 195(1) of the Constitution states:

“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 maximize 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.”

9.1 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.



9.2 Understanding Fraud

To effectively combat fraud, theft, and corruption, it is essential to understand their nature and impact. Fraud involves any act of dishonesty that causes harm or misleads others, often involving the misuse of public resources.

9.3 Defining Fraud

In South African law, fraud is defined as “the unlawful and intentional making of a misrepresentation that causes actual or potential prejudice to another.” In this document, “fraud” is used in its broadest sense to include all forms of economic crime and dishonesty, encompassing fraud, theft, and corruption.

Fraud, therefore, is any act of deception by a public servant or external party that misleads others to gain a benefit that should serve the public interest.

9.4 Forms of Fraud

Fraud within the Department can manifest in various forms, each undermining the integrity and effectiveness of public service. Recognising and understanding these forms are crucial for effective prevention and response. The key forms include:

- **Management Fraud:** Involves senior management engaging in fraudulent activities, potentially in collusion with external entities.
- **Employee Fraud:** Pertains to public servants committing fraudulent acts, which may include collusion with third parties outside the Department.
- **Fraudulent Reporting:** Involves deliberate misstatements or omissions in financial or other reports designed to deceive stakeholders. This form of fraud can lead to significant financial mismanagement and loss of public trust.
- **Maladministration or Financial Misconduct:** Includes improper handling or reporting of financial transactions, misuse of funds, or assets.
- **Irregular or Wasteful Expenditure:** Any expenditure that is unauthorised, not in accordance with regulations, or considered wasteful, as defined by the Public Finance Management Act (PFMA).
- **Unauthorized Disclosure of Confidential Information:** Involves the illegal or unethical release of sensitive information, either intentionally or through negligence. Such breaches can compromise national security and public safety.
- **Gifts and Bribery:** Accepting, offering, or requesting gifts or bribes from contractors, suppliers, or other third parties in exchange for preferential treatment or business.
- **Asset Theft:** The unlawful taking of Departmental funds, supplies, or other assets for personal gain. This form of fraud directly depletes public resources intended for community development and services.

Understanding these forms of fraud is essential for implementing effective prevention, detection, and response strategies, thereby safeguarding public resources and maintaining the integrity of the Department.

9.4.1 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.

9.4.1.1 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.

9.4.2 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.

9.4.3 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

9.4.4 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:

- 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.

9.5 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.



9.6 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

9.7 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.

9.7.1 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.

9.7.2 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 the 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.

9.8 FRAUD PREVENTION STRATEGY

9.8.1 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.

9.8.2 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.
- d) 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.

9.8.3 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.

9.8.4 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.

9.8.5 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 about the 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.

9.8.6 Ethics Infrastructure

The Public Sector Integrity Management Framework (PSIMF) has been established to create a robust Integrity Framework that aligns with existing regulatory measures governing ethics and integrity in the public sector. The framework is designed to achieve the following objectives:

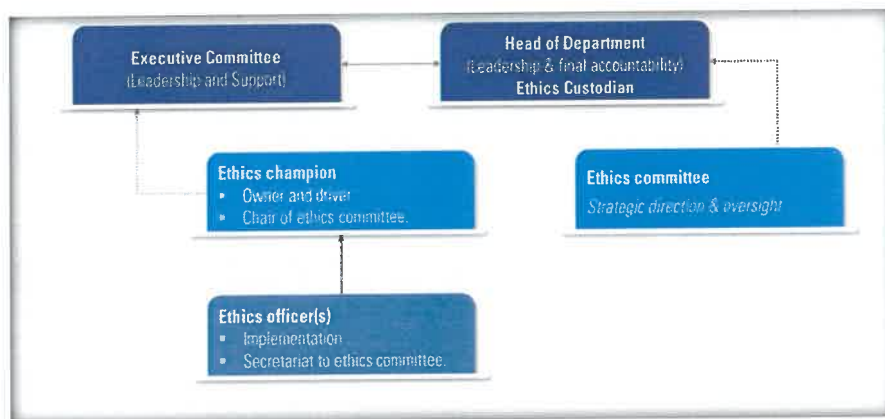
- **Strengthen Existing Measures:** Enhance the current systems and protocols that regulate ethical conduct and probity within the public service.



- **Build Capacity to Prevent Corruption:** Increase the capacity of the Department to proactively prevent corruption through improved policies, training, and awareness programs.
- **Monitor and Evaluate Compliance:** Establish comprehensive mechanisms for monitoring, evaluating, and ensuring compliance with ethical standards and regulations.
- **Enforce as a Deterrent:** Implement enforcement strategies to act as a deterrent against unethical behavior, ensuring accountability and promoting a culture of integrity.

This infrastructure is vital in fostering an ethical culture within the Department, ensuring that all employees and stakeholders adhere to the highest standards of integrity, and ultimately contributing to the reduction of corruption and fraud within the public service.

The **Public Sector Integrity Management Framework (PSIMF)** provides essential guidelines for structuring the **Ethics Infrastructure** within the Department. To ensure effective implementation of ethical practices and anti-corruption initiatives, the Department shall consider the following actions:



1. Designating an Ethics Champion at the Executive Level:

- Appoint an Ethics Champion with the authority to lead and drive the Department's ethics and anti-corruption initiatives at the highest leadership level.

2. Establishing an Ethics Committee (or utilising an existing one):

- Form an Ethics Committee responsible for shaping the Department's ethics strategy and providing oversight on integrity management activities.

3. Creating an Ethics Office:

- Establish a dedicated Ethics Office, positioned at a high level within the Department, to manage the day-to-day operations of the ethics management program. Responsibilities of the Ethics Office will include:
- Overseeing the entire ethics program
- Providing advice and regular reports on ethical matters
- Conducting investigations and monitoring ethics compliance
- Managing audits and assessments related to ethics
- Lead corporate social responsibility and integrity functions

4. Appointing Ethics Officer(s) and Defining Responsibilities:

- Appoint Ethics Officer(s) with clearly defined responsibilities, including:
- Promoting integrity and ethical behavior within the Department
- Offering advice to public servants on ethical issues
- Ensuring the integrity of the Department's policies, procedures, and practices
- Identifying and reporting unethical conduct and corrupt activities to the Head of Department (HOD)



- Managing conflicts of interest, such as:
- Reviewing financial disclosures of public servants
- Overseeing applications for external remunerative work
- Maintaining a register of public servants under investigation or disciplined for unethical behavior

5. Developing and Implementing Awareness Programs:

- Design and implement awareness programs to educate all officials on ethics, good governance practices, and anti-corruption measures, ensuring that all employees understand and adhere to ethical standards.
- By adhering to these guidelines, the Department will enhance its commitment to ethical conduct and provide a clear structure for managing and promoting integrity and accountability.

9.8.7 Fraud Risk Assessments

The Department recognizes the diverse business risks arising from both internal and external environments. To address these risks, the Department conducts **Fraud Risk Assessment** workshops where potential risks are identified, assessed, and prioritized. Once the major risks are identified, the team designs strategies to prevent fraud in these areas.

Key components of this approach include:

- **Fraud Risk Register:** The identified fraud risks are documented in the Fraud Risk Register, which is maintained by the **Internal Audit** team. This register is reviewed and reported to the **Audit Committee** and senior executives.
- **Risk Ownership:** Specific individuals or departments are assigned as "Risk Owners" to ensure that each risk is actively managed and mitigated.
- **Action Plans:** Proposed actions are developed for all identified risks, including those assessed as lower in risk but still requiring mitigation. These actions are reviewed and evaluated by **senior management** before they are implemented.
- **Fraud and Ethics Risk Register:** This document is regularly updated and serves as a comprehensive tool to track and mitigate fraud and corruption risks. It prioritizes risks and outlines the necessary actions for their mitigation.
- **Annual Review and Updates:** On an annual basis, management presents the updated fraud risks and corresponding mitigation strategies to the **Audit Committee**. Risks that remain inadequately managed and carry material potential impact are specifically addressed, especially if new systems are required to manage them.
- **Evaluation of Effectiveness:** The effectiveness of the fraud prevention and mitigation controls is assessed by **Internal Audit** to ensure that these measures are effective in the evolving risk landscape.

This structured approach ensures that fraud and ethics risks are continuously identified, prioritised, and managed, with transparent reporting and review processes to foster accountability and reduce exposure to fraud and corruption.

9.8.8 Human Resource Policies and Systems

The Department is committed to developing robust human resource systems, policies, and procedures that promote integrity, prevent fraud, and combat corruption. The key components of these policies are as follows:

a) Recruitment - Employee Screening Procedures



Recruitment processes will adhere to a transparent procedure, ensuring that all appointments are made based on merit and after proper recommendation. Any person involved in decision-making who may have a conflict of interest must declare it in writing to the Human Resource Department and recuse themselves from further involvement. If it is later found that a decision-maker failed to declare a conflict of interest, they may face disciplinary actions. All members of the Selection and Short-listing committee must adhere to confidentiality and conflict of interest disclosure clauses.

b) Pre-employment Screening

Vetting and screening are essential practices to identify potential risks and prevent corruption within the Department. 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. This helps ensure that only qualified, trustworthy individuals are employed, minimizing the risk of unethical behaviour.

c) Employee Induction Training

Induction training provides a crucial opportunity to instill ethical standards, fraud awareness, and integrity from the onset of an employee's tenure. All new officials, including contractors and temporary employees, must undergo induction within the first three months. This training will incorporate the Department's Fraud Prevention Strategy, Code of Conduct, Disciplinary Code, and fraud awareness initiatives. Corporate Services will be responsible for coordinating the induction process.

d) Obligatory Leave Periods

To reduce the risks of fraud and non-compliance due to over-worked employees, all officials are entitled to at least 22 days of annual leave, which must include 10 consecutive days of compulsory leave. Heads of Department are encouraged to ensure appropriate scrutiny and supervision for employees who may not take leave due to work commitments, ensuring the continued integrity of internal controls.

e) Probation

Probationary periods will be mandatory for all new full-time employees. During this period, the employee will undergo relevant vetting and screening procedures. Vetting will be conducted both at the beginning and throughout the probationary period to ensure the employee meets the required ethical standards before final confirmation of their employment.

f) Exit Procedure and Return of Assets

The Department's exit procedure ensures that all assets are returned and all electronic information is secured when an employee leaves the Department. The employee must complete an exit clearance form and participate in an exit interview. Any suspicious activity or misconduct identified during this process will be reported to senior management for further investigation. This step helps mitigate fraud risks associated with employee exits.

g) Remunerative Work Outside the Public Service

Any public servant considering external business activities or directorships must obtain prior written approval from the MEC responsible for the Department. The MEC will assess whether the external work may interfere with the employee's duties. The assessment will include the nature of the work, the time commitment required, and the employee's performance record. The application process will be extended from 30 days to allow sufficient time for review and approval.

h) Prohibition of Corrupt Individuals from Public Service

To maintain the integrity of the public service, individuals found guilty of corruption will be prohibited from working in the public sector or contracting with the government for a period of up to 5 years, as determined



by the presiding officer. The prohibition will be recorded in employment systems and publicly published. The Department will also consult a centralised register to screen potential contractors and will require contractors to declare any previous convictions related to corruption.

i) Procurement Policies and Procedures

The Department is committed to developing and maintaining procurement policies and procedures that incorporate measures to prevent fraud and corruption. These procedures will ensure fairness, transparency, and accountability in all procurement activities.

j) Vendor Due Diligence Procedures

All suppliers will be registered on the Department's database, and due diligence will be conducted both before and during the procurement process. This ongoing process helps ensure that all vendors meet the necessary standards of integrity and that their business practices align with the Department's ethical requirements.

The following procedures may be performed:

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

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.



a) 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.

b) 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.

i. 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.



c) 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

Heads of Department and Senior Management

- 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.

All public servants

- 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

All public servants

- 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.

i. 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.

d) 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.

- a) 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.
- b) 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.

e) 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.

f) 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
10. 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 encourage 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



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.

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.



D: 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.

E: POLICY REVIEW

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

F: APPROVAL

The Fraud Prevention Strategy is approved as follows:

DESIGNATION	NAME	SIGNATURE	DATE
RECOMMENDATION			
Risk Management Committee Chairperson	Mr. M.I. Buwa		18 March 2025
Approval			
Head Of Department	Mr. M.I. Kgantsi		25/04/25

