



the dti

Department:
Trade and Industry
REPUBLIC OF SOUTH AFRICA

Fraud Prevention Policy and Strategy



Document History

REVISION NUMBER: 1
COMPILED BY: B Arumugam
REFERENCE NUMBER: the dti Fraud Prevention Policy and Strategy
DATE COMPLETED: 1 September 2009

<i>Version</i>	<i>Date</i>	<i>Revision description</i>
1.0		Draft for approval by OPSCOM after which it will be known as version 1.0
1.0		Approved by OPSCOM on

Part I

FRAUD PREVENTION POLICY

1. INTRODUCTION

- 1.1 The Fraud Prevention Policy represents the commitment of **the dti** to effective fraud risk management. It also requires the commitment, cooperation and involvement of all staff in preventing, detecting and responding to all instances of fraud.
- 1.2 There is a continuing need to raise staff awareness of their responsibility to safeguard public resources against the risk of fraud. The overall purpose of the Fraud Prevention Policy ("FPP") is to detail responsibilities regarding the prevention of fraud in **the dti**. The procedures to be followed in the event of fraud being detected or suspected are detailed in the Fraud Prevention Strategy. Both documents deal with fraud and loss within **the dti** and its agencies. Reporting arrangements also apply to monies for which **the dti** is accountable but expended outside the department.
- 1.3 **The dti** requires all staff, at all times, to act honestly and with integrity in safeguarding the public resources for which they are responsible. Fraud is an ever-present risk to the resources and must be a concern to all staff members.
- 1.4 **The dti** will not tolerate any level of fraud and corruption; consequently, **the dti's** departmental policy is to thoroughly investigate all suspected fraud and allegations (anonymous or otherwise) and where appropriate, refer to SAPS at the earliest juncture. **The dti** is also committed to ensuring that opportunities for fraud and corruption are reduced to the lowest possible level of risk.

2. SCOPE AND APPLICATION

- 2.1 This Policy applies to all of **the dti's** divisions and their respective business units enterprise-wide. It also applies to all its agencies.
- 2.2 For the purpose of this Policy, the term "staff" refers to all its employees, whether permanent or on contract, as well as to consultants and contractors conducting activities on-site or otherwise under the control of **the dti**.
- 2.3 Fraud committed against **the dti** is a criminal offence under various provisions of legislation. Fraud also constitutes serious misconduct under **the dti** Disciplinary Code of Conduct.

3. FRAUD DEFINED

3.1 Legal definition:

Fraud is any **unlawful, intentional misrepresentation** of facts (distortion of truth) calculated to **prejudice** another. The use of the term is in its widest meaning and is intended to include all aspects of economic crime and acts of dishonesty.

- **Unlawfulness:** The action must be seen to be wrong in the eyes of society
- **Intention:** Deceit or intention to prejudice
- **Misrepresentation:** An incorrect statement of fact or law by one person to another (words, conduct, silence)
- **Prejudice:** Some sort of harm to another (proprietary, non-proprietary, actual, potential).

3.2 Causes of Fraud:

Fraud comes in many forms, ranging from embezzlement to identity theft, and while the list of possible incidences is not exhaustive, there are certain warning signals which can indicate the occurrence of fraud and definite situations which lend themselves to this crime.

Fraud is most often a crime of opportunity committed by people who face overwhelming financial pressures or simply greed.

3.3 Examples of what constitutes fraud

The following list, whilst not exhaustive, provides examples of the types of conduct that would be included within **the dti's** definition of fraud:

- a) Theft of property eg. stationery, cash, and equipment, through wilful misrepresentation.
- b) Unlawful or unauthorised release of confidential information.
- c) Dishonest use of intellectual property of **the dti** or of its electronic systems.
- d) Knowingly making or using forged or falsified documents.
- e) Dishonest use of **the dti's** computers, vehicles, telephones, credit cards, and other property or services.
- f) Fabrication, falsification or plagiarism of research or scholarly work.
- g) Falsifying invoices for goods or services.
- h) Dishonestly using purchase or order forms to gain a personal benefit.
- i) Receiving or giving kickbacks or secret commissions to or from third parties.
- j) Falsifying travel, subsistence and petty cash claims.

3.4 Situations that could lead to Fraud

- a) Failing to disclose financial interests outside of employment with **the dti**.
- b) Failing to acknowledge and avoid conflicts of interest.
- c) Failing to observe the prescripts of the Supply Chain Management System
- d) Accepting inappropriate gifts from suppliers
- e) Employing family members or close friends
- f) Operating a private business during working hours
- g) Poor personal financial management and indebtedness to creditors by a **dti** official.
- h) Lack of personal discipline by a **dti** official.
- i) Inadequate or ineffective internal systems of control within **the dti**.
- j) Inconsistent or ineffective treatment of misconduct involving dishonesty by the organisation and its management.

3.5 Corruption defined

Whilst this Policy is primarily focused on the identification and eradication of Fraud, it is important to reflect on the relationship between Fraud and Corruption, as Fraud is a legal offence created by law and defined as such, whereas Corruption is a broader offence which has as its essence a breach of ethical conduct. Corruption is defined as:

“giving or offering; receiving or agreeing to receive; obtaining or attempting to obtain any benefit which is not legally due to or by a person who has been charged with a duty or power by virtue of any employment, to do any act or omit to do any act in relation to that power or duty.”

4. POLICY PRINCIPLES

4.1 the dti's attitude to fraud

- a) **The dti** has a *zero tolerance* attitude to fraud.
- b) **The dti** is committed to minimising the incidence of fraud through the development, implementation and regular review of fraud prevention, detection and response activities, as well as through periodic risk assessment exercises.

4.2 the dti's approach to fraud

- a) **the dti** will ensure that all staff members are aware of the fraud reporting procedures and actively encouraged to report suspected fraud through the appropriate channels.
- b) **the dti** has adopted a clear framework and approach to fraud prevention, the full details of which appear in its Fraud Prevention Strategy, which is attached as Part II hereto. In particular, the following fraud control strategies may be implemented by **the dti**:

Prevention Strategies	Detection Strategies
▼	▼
Ethics Framework - Code of Conduct Guidelines	Data Analysis
Fraud Prevention Strategy (including allocation of fraud prevention responsibilities)	Management Reports reviews
Fraud & Ethics Awareness Training	Fraud & Ethics Awareness Training
Fraud Risk Assessments	Clear reporting channels
Robust internal controls	Whistleblower protection
Pre-employment screening	Internal auditing

- c) All information received by **the dti** in relation to suspected fraudulent conduct will be collected, classified and handled appropriately having regard to privacy, confidentiality, legal professional privilege, and the requirements of natural justice.

5. STATEMENT OF ATTITUDE TO FRAUD

5.1 Fraud has the potential to damage the reputation of **the dti** and have a detrimental effect on the resources available to promote **the dti's** objectives. Accordingly, **the dti** has adopted a *zero tolerance* to fraud and is committed to minimising the incidence of fraud through the development, implementation and regular review of fraud prevention, detection and response activities. Each activity contributes to an environment where risk is managed, through sound internal controls, and ethical practices.

5.2 To achieve its fraud prevention objectives, **the dti** will:

- a) identify fraud risks and review and update the Fraud Prevention Policy and Strategy every two years;
- b) provide fraud awareness training to those staff who are considered to be in positions that require fraud awareness training;
- c) ensure all staff are aware of **the dti's** Fraud Prevention Policy;
- d) encourage and promote professional and ethical business practice;
- e) aim to identify fraud through regular review of **the dti's** operations;
- f) clearly communicate how suspected instances of fraud may be reported;
- g) investigate alleged or suspected instances of fraud using qualified personnel and professionals with experience in investigation techniques;
- h) take appropriate action to deal with instances of actual, suspected or alleged fraud, including prosecution of persons and/or organisations for fraud offences where and when appropriate; and
- i) use all available avenues to recover money or property lost through fraudulent activity.

6. EXPECTATIONS OF STAFF

- a) Staff are expected to act in a professional and ethical manner, follow legal requirements, have due care for **the dti** property, and maintain and enhance the reputation of **the dti**.
- b) Staff are expected to remain vigilant to any suspected fraudulent behaviour that may be occurring around them and are expected to fully cooperate with any investigations and the implementation of fraud prevention strategies.
- c) Staff who become aware of suspected fraudulent conduct must report the matter in accordance with this Policy, and must thereafter retain strict confidentiality on such possible fraud incidents of which they have knowledge.
- d) Any failure by staff to comply with this Policy may result in disciplinary action against them.

7. REPORTING PROCEDURE IF FRAUD IS SUSPECTED

Responsibility: All staff

- a) In the first instance, report any suspected fraud incident to your relevant line manager.
- b) If, for any reason, you feel that reporting the incident through the relevant line manager would be inappropriate, report the matter directly to the Director : Corporate Governance, GSSSD or to the Director : Forensic and Compliance Audit, ODG.
- c) If, for any reason, you feel that reporting the incident internally would be inappropriate, then you may report the matter directly to the National Anti-Corruption Hotline (NACH) on **0800 701 701**. Such reports may be made confidentially, if desired.
- d) Every staff member is required to act in good faith and reasonably in reporting alleged fraudulent activity.
- e) All such reports made in accordance with the Whistleblowers Policy will enjoy the protection against victimisation provided for by the Protected Disclosures Act.



Part II

FRAUD PREVENTION STRATEGY

In implementing the policy and in combating fraud, **the dti** will embark in the following techniques:-

1. PREVENTION

1.1 Embedding an ethical culture

As personal ethics influences a person's behaviour and conduct in the workplace, a fundamental strategy in controlling the risk of fraud is the development and maintenance of a sound ethical culture, underpinned by effective and continuous communication and example-setting by management.

The attitude of **the dti** to ethical conduct in relation to its values as an organization will be expressed in its Ethics Framework document, which will set out the various efforts being made by **the dti** to ensure that there is a culture of integrity in the department. Amongst others:

- a) The Risk Management Unit (RMU) will in consultation with HR develop **the dti's** code of conduct.
- b) The RMU and HR will ensure that all employees confirm their understanding of the code of conduct by attesting their signature.
- c) The RMU will conduct workshops on the promotion of ethical behaviour in the workplace.
- d) There must also be a culture of rewarding ethical conduct by way of public recognition, while conduct that is unethical must be actively discouraged by way of reinforcing good behaviour and transparently condemning examples of unacceptable behaviour.

1.2 Fraud awareness training

Generally, a significant proportion of fraud goes undetected because of the inability to recognise the early warning signs of fraudulent activity or because they are unsure how, when and to whom they should report their suspicions. Accordingly, **the dti** has incorporated fraud awareness training to assist in raising the general level of awareness amongst staff.

An awareness of the risk of fraud and fraud prevention techniques will be fostered by:

- a) ensuring that all new staff are made aware of the Fraud Prevention Strategy during induction;
- b) ensuring that all staff that are considered to be in positions requiring training attend fraud awareness training;
- c) ensuring staff are aware of the ways in which they can report allegations or concerns regarding alleged fraud or alleged unethical conduct; and
- d) encouraging staff to report any suspected incidents of fraud.

1.3 Assessment of fraud risks

- a) The RMU will conduct risk assessment workshops after every 12 to 18 months.
- b) Risks that may be regarded as fraud or corruption related will be addressed by implementing the Fraud Prevention Strategy.

1.4 Internal control

Internal controls are often the first line of defence against fraud and corruption, and they are essential elements in the overall anti-fraud and corruption strategy. **the dti** will ensure the maintenance of a strong internal control system and the promotion and monitoring of a robust internal control culture.

the dti will promote an internal control culture through a process of:

- a) Example-setting by management (“walking the talk”);
- b) Mapping of business processes to ensure that controls are built in and risks are managed;
- c) Regular communication of the importance of internal controls;
- d) Including adherence to internal controls as part of the performance management framework;
- e) Once fraud risks are identified during risk assessments, appropriate control measures must then be determined and implemented;
- f) If circumstances change and specific risks are identified that cannot adequately be managed by means of ordinary controls, specific forensic controls to address such risk will be instituted.

1.5 Pre- Employment Screening

- a) Pre-employment screening is an effective means of preventing fraud, such as falsifying qualifications or employment history. It can also identify previous criminal convictions for offences of dishonesty.
- b) The pre-employment screening will be carried out for all appointments; evidence of such screening will be maintained by HR unit.
- c) The screening will be performed by a person / people nominated by the HR.
- d) In cases where appropriate, security vetting in terms of the requirements of the National Intelligence Agency (NIA) will be conducted by the Vetting Office of Accommodation Management Services.

1.6 Disclosure of interests

- a) All SMS members will be required to disclose their financial interests to the RMU on an annual basis as per the dti Conflicts of Interest Policy.
- b) All staff members other than SMS members are required to disclose their financial interests to their Chief-Directors or their Deputy Directors-General.
- c) It is the prerogative of **the dti** to check the correctness of any information so disclosed.
- d) Failure to disclose fully all personal interests, or disclosing in such a manner as to mislead or misrepresent one’s true interests, shall not be tolerated and will incur such disciplinary action as will be deemed appropriate.

2. DETECTION

It is recognised that, despite the existence of a fraud prevention program, fraud may still occur. Accordingly, it is necessary for mechanisms to be in place that are aimed at detecting and dealing with fraud as soon as possible after it has occurred.

2.1 Management accounting reporting review

Using relatively straightforward techniques in analysing **the dti's** management accounting reports, trends can be examined and investigated which may be indicative of fraudulent conduct. **the dti** currently adopts appropriate management accounting reporting reviews.

The following sources will be used to ensure the detection of fraud in Finance section:

- a) Audit findings
- b) Register of irregular expenditure
- c) Register of fruitless expenditure
- d) Annual report and Annual Financial Statements.

2.2 Identification of early warning signs

Identification and acting on early warning signs of fraudulent activity is an important part of early fraud detection. The key to achieving an early warning capability is awareness. The fraud awareness training program, referred to in Section 4.2 of the FPP, will therefore include the identification of early warning signs or "red flags" for suspected fraud and how to respond if they are identified.

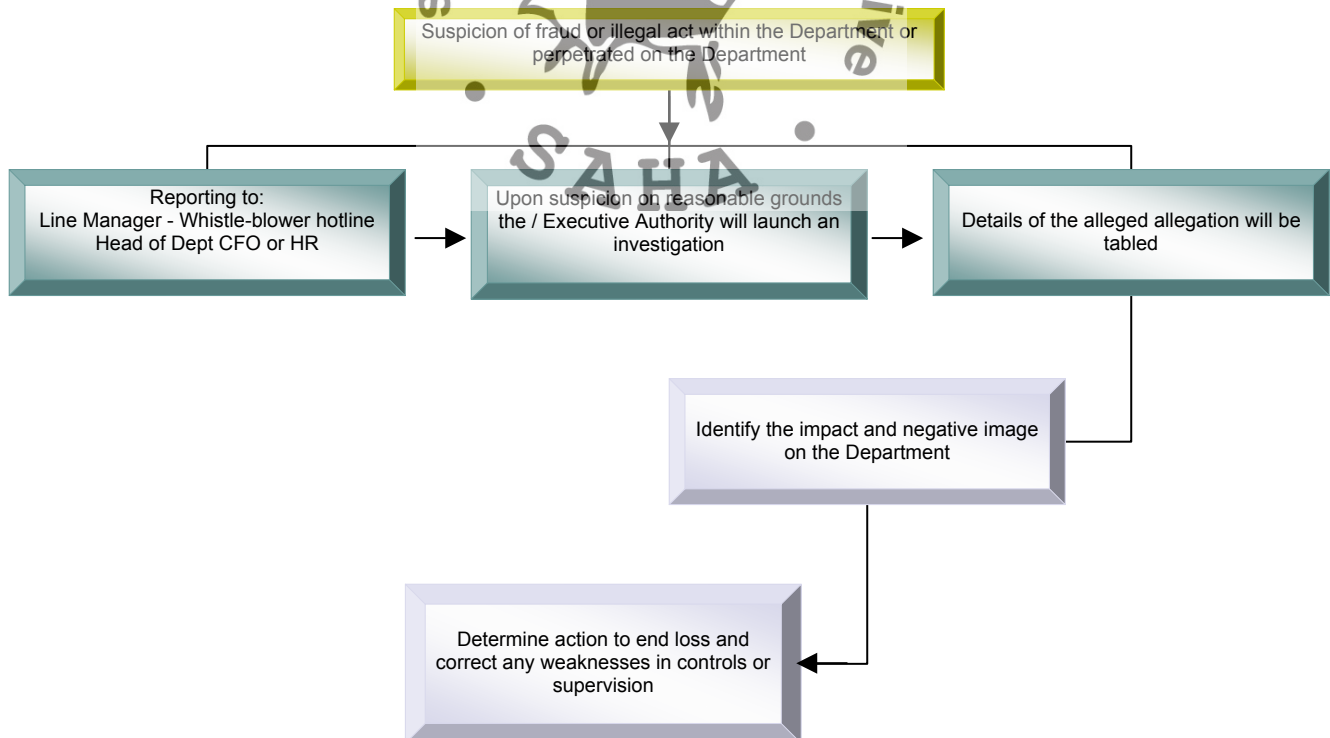
All staff members, particularly managers, should be aware of their responsibility to remain vigilant to identify and report any suspected fraudulent activity.

2.3 Reporting instances of fraud

Every staff member who becomes aware of suspected fraudulent conduct is required to report the matter in accordance with this procedure:

- a) In the first instance, report any suspected fraud incident to their relevant line manager.
- b) If, for any reason, they feel that reporting the incident through the relevant line manager would be inappropriate, report the matter directly to the Director : Corporate Governance, GSSSD or to the Director : Forensic and Compliance Audit, ODG. They may also report to the Head of Human Resources (HR), or to the Chief Financial Officer (CFO), or to the head of the appropriate division. Such reports may be made confidentially, if desired.
- c) If, for any reason, they feel that reporting the incident internally would be inappropriate, then they may report the matter directly to the National Anti-Corruption Hotline (NACH) on **0800 701 701**. Such reports may be made confidentially, if desired.
- d) Every staff member is required to act in good faith and reasonably in reporting alleged fraudulent activity.
- e) Every staff member is also required to maintain strict confidentiality on any suspected fraud matter of which they have knowledge.

The diagram below depicts the procedure to report fraud:



2.4 Whistleblower protection

- a) Whistle-blowing is about raising a concern about malpractice within an organization. It is a key tool for promoting individual responsibility and organisational accountability.
- b) However, one of the key obstacles to whistle-blowing is the fear of being intimidated or victimised for identifying or exposing fraudulent, corrupt or unethical practices witnessed in the workplace.
- c) In order to encourage individuals to come forward with such information without the fear of victimisation, **the dti** has institutionalised the protection afforded to whistle-blowers by the Protected Disclosures Act by approving its own Whistle-blowing Policy.

2.5 National Anti-corruption Hotline (NACH)

- a) **the dti** subscribes to the National Anti-corruption Hotline administered by the Department of Public Service for all public institutions. The hotline number is **0800 701 701** and it has been publicized throughout **the dti**.
- b) This anti-fraud reporting facility complements and underpins the commitment of **the dti** to fighting fraud and corruption. The key benefits of the tip-off reporting facility are:
 - (i) Independent management by a third party
 - (ii) Confidential reporting
 - (iii) Operates throughout the year, including after hours
 - (iv) Technology-driven
 - (v) Secure (people, system and data)
 - (vi) Reporting by telephone, fax, post or e-mail
 - (vii) Continual internal marketing and top management support
 - (viii) A multi-language capability
 - (ix) Promotes good governance
 - (x) It is an easy way of promoting a culture of honesty and integrity.

2.6 Physical security

At all times, there is a physical presence of security officials on duty throughout **the dti** campus. There are also surveillance cameras located at strategic points, and these visible security measures serve a role in creating and sustaining a deterrent environment for the commission of wrongful activities.

3. RESPONSE

3.1 Forensic Investigation

- a) In the event where fraud or corruption is detected or suspected, Internal Audit (Forensic Investigation) will ensure that the case is fully investigated, and a progress report is presented at the Pre-risk meeting before each RMC meeting.
- b) These reports are handled with strict sensitivity and confidentiality.
- c) All suspected fraud cases will be handled consistently and without regard to positions held or length of service by the parties being investigated.

3.2 Disciplinary Action

- a) Subsequent to full investigation, **the dti** will take legal and / or disciplinary action in all cases where it is considered necessary and appropriate.
- b) Any member of staff found guilty of a criminal act involving dishonesty will be considered to have committed a serious disciplinary offence and may be dismissed from **the dti** on the grounds of misconduct.

- c) **the dti** will also use a “name-and-shame” approach as a deterrent to other staff members to ensure that such behaviour is not repeated or encouraged.

3.3 Reviewing systems and procedures (post fraud)

In each instance where fraud is detected, **the dti** will re-assess the adequacy of the internal control environment (particularly those controls directly impacting on the fraud incident and potentially allowing it to occur) and actively plan and implement improvements where required. Where improvements are required, they will be implemented as soon as practicable.

3.4 Recovery of money or property lost through fraud

the dti will actively pursue the recovery of any money or property lost through fraud after considering all relevant issues, which will include instituting criminal prosecution.

4. RESPONSIBILITIES

4.1 The Accounting Officer / the Director-General

In terms of Part 2: Responsibilities of Accounting Officers, Section 38(1) of the Public Finance Management Act No 1 of 1999 (as amended by Act 29 of 1999), the accounting officer is responsible for establishing and maintaining a sound system of internal control that supports the achievement of departmental policies, goals and objectives.

The Director-General as accounting officer lawfully delegates this responsibility to the Director: Corporate Governance as the official assigned to manage the Corporate Governance function in **the dti**, which is the custodian of the Fraud Prevention Policy and Strategy for **the dti**. However, despite this delegation to the Director: Corporate Governance for implementation, the Director-General will remain accountable and will not in any way abdicate his responsibilities in terms of the PFMA.

4.2 The Executive Board (Exbo) and Senior Management Service (SMS)

The Senior Management team must ensure that the Fraud Prevention Policy and Strategy are effectively implemented, while Exbo must exercise an oversight function to ensure that appropriate action is taken against non-compliance.

4.3 The Risk Management Unit

The Risk Management Unit (RMU) within the Corporate Governance Directorate is the custodian of the Fraud Prevention Policy and Strategy within **the dti**. The responsibilities of this Unit include:-

- a) Developing a Fraud Risk profile, and undertaking a regular review of the fraud risks associated with each of the key organisational objectives, in relation to operational risks identified as well as the results of forensic audits;
- b) Managing and revising the Fraud Prevention Policy and Strategy;
- c) Assisting the Human Resources business unit with the appropriate pre-employment screening measures;
- d) Establishing appropriate mechanisms for ensuring proper awareness, and ensuring that proper anti-fraud training is provided for all staff;
- e) Ensuring the reporting of fraud risk issues, and escalating to Exbo to ensure that appropriate action is taken against non-compliance or failure to report fraud; and
- f) Liaising with both the Risk Management Committee (RMC) and Audit Committee (AC), which committees will:-
 - I. ensure that fraud prevention issues are addressed and dealt with in an effective manner ensuring “zero-tolerance” on fraud and corruption.

4.4 Internal Audit

The Internal Audit function does not bear a direct responsibility for the prevention or detection of fraud; however, they have to ensure that the controls for prevention are feasible for the maintenance of a “zero tolerance” to crime approach. The Internal Audit will be responsible for the investigation of all cases that are related to fraud, corruption and forensics. In the course of their work, it is foreseeable that they may inadvertently unearth fraudulent activities, and in such instances, the normal investigative processes will be adopted.

4.5 Staff Responsibilities

Every staff member has a duty to ensure that public funds are safeguarded, and therefore everyone is responsible for:-

- a) Being vigilant to the possibility that unusual events or transactions could be indicators of fraud, and alerting their superiors or “blowing the whistle” by calling the national anti-corruption hotline on **0800 701 701** if fraud is suspected, attempted or committed. The Conflicts of Interest and the Whistle-blower policies protect the rights of staff who report wrongdoing;
- b) Assisting in any investigation by making available all relevant information, by co-operating in interviews and if appropriate providing a witness statement;
- c) Conducting himself / herself in an ethical and moral manner;
- d) Adhering to the Public Service Code of Conduct;
- e) Attending all the awareness campaigns and anti-fraud trainings that will be conducted and facilitated by the Corporate Governance Unit at least twice annually.

5. LEGISLATIVE PRESCRIPTS

a) Public Finance Management Act, No 1 of 1999 as amended by Act 29 of 1999 (PFMA):

Sections 76 (4)(d) and 77 of the PFMA state that the Audit Committee and the Accounting Officer must facilitate a risk assessment to determine the material risks to which the institution may be exposed and to evaluate the strategy for managing these risks. The strategy must be used to direct audit efforts and to determine the skills required to manage these risks.

Part 2: Responsibilities of Accounting Officers, Section 38(1) of the Public Finance Management Act No 1 of 1999 (as amended by Act 29 of 1999) states that the accounting officer is responsible for establishing and maintaining a sound system of internal control that supports the achievement of departmental policies, goals and objectives. Specifically:

1. The accounting officer:-
 - a) Must ensure that the department has and maintains:-
 - I. Effective, efficient and transparent systems of financial and risk management and internal control;
 - II. A system of internal audit under the control and direction of an audit committee complying with and operating in accordance with regulations and instructions prescribed in terms of sections 76 and 77.
 - b) Is responsible for the effective, efficient, economical and transparent use of the resources of the department;
 - c) Must take appropriate steps to:-
 - I. Prevent unauthorised, irregular and fruitless and wasteful expenditure and losses resulting from criminal conduct;
 - d) Is responsible for the management, including the safeguarding and the maintenance of the assets, and for the management of the liabilities of the department;

- h) Must take effective and appropriate disciplinary steps against any official in the service of the department who:-
- I. Contravenes or fails to comply with a provision of the PFMA;
 - II. Commits an act which undermines the financial management and internal control system of the department; or
 - III. Makes or permits an unauthorized expenditure, irregular expenditure or fruitless and wasteful expenditure.

b) King Report on Corporate Governance II:

The risk management system should incorporate mechanisms to deliver the following:

- A demonstrable system of dynamic risk identification
- A demonstrable system of risk mitigation activities
- A system of documented risk communications
- A system of documenting the costs of non-compliance and losses
- A documented system of internal control and risk management and
- A register of key risks that could affect relevant stakeholders' interests.

c) Treasury Regulations, section 3.2.1:

- The Accounting Officer must ensure that a risk assessment is conducted regularly so as to identify emerging risks of the institution.
- A risk management strategy, which must include a fraud prevention plan, must be used to direct internal audit efforts and priority, and to determine the skills required of managers and staff to improve controls and manage these risks. The strategy must be clearly communicated to all officials to ensure that the risk management strategy is incorporated into the language and culture of the institution.

d) Corruption Act, No 94 of 1992:

Section 1 of this Act stipulates that any person that corruptly gives or offers or agrees to give any benefit, receives, or obtains or agrees to receive any benefit, to commit or omit any act, is guilty of a criminal offence.

e) Promotion of Access to Information Act, No 2 of 2000:

- (i) In terms of the Promotion of Access to Information Act, No 2 of 2000, **the dti** must delegate responsibility to deal with requests for information to a designated Information Officer.
- (ii) A person, who with intent, denies a right of access to information, and destroys, damages, alters conceals or falsifies records, commits an offence and is liable on conviction, to a fine or imprisonment.
- (iii) The Act further makes provision for procedure in terms of which employees in both the private and the public sector may disclose information regarding unlawful or irregular conduct, by their employers or peers. It also provides for the protection of employees who make a disclosure.

f) Protected Disclosure Act, no 26 of 2000:

In accordance with the Protected Disclosures Act, No 26 of 2000, staff members of the organisation disclosing any acts of maladministration, fraud, or corruption are protected from any occupational detriment. Disclosures can be made to the employer of the organisation delegated by the accounting officer to handle complaints, Minister of Labour, the Public Protector or the Auditor-General.

g) Prevention and Combating of Corrupt Activities Act, 2004 (Act No 12 of 2004):

- (i) Sections 4 and 34 of the Act make it an offence for a public official to accept any form of gratification from another person, whether for his / her benefit or the benefit of another person.
- (ii) The Act places a duty on any person holding a position of authority and who knows or reasonably ought to have known or suspected that any other person has committed certain corrupt transactions, to report it.
- (iii) Such corrupt transactions include theft, fraud, extortion, forgery or uttering a forged document involving an amount of R100 000, 00 or more.
- (iv) Persons holding positions of authority are defined to include, *inter alia*, Directors-General of national and provincial departments, public officers in senior management service (SMS), secretaries, directors and managers of companies, and CEOs or equivalent of agencies, boards, institutions, funds, or entities.

h) King Report on Corporate Governance III (draft):

The third Report on Governance in South Africa (King III) was published by the Institute of Directors (IoD) in draft format for written comments. The King III report will become effective on 1 March 2010 and until then, the current King II report will apply.

There is, however, an important departure from the previous requirement that companies had to 'comply and explain' with regard to the code. The requirement is now that companies have to 'apply and explain' the code. This is a move away from the so-called 'tick box compliance' approach to an approach which requires more consideration of what is actually done to implement the code, and in this regard it is wise for the dti to bring regulations for such a shift of emphasis.

The report also states that internal audit should be risk-based, and internal auditors should furnish an annual assessment to the audit committee on the adequacy of internal controls. In order to give substance to the endorsement by directors of the internal controls in a company, the audit committee needs to report fully to the board.

6. CONCLUSION

- a) It is appreciated that the circumstances of individual fraud will vary. However, the dti takes fraud very seriously and will ensure that all cases of suspected fraud are vigorously and promptly investigated and that remedial action is taken where appropriate.
- b) Every staff member should be fully aware of his / her responsibility to protect public funds and assets and as such, should always be alert to the potential for fraud.
- c) Any queries in connection with this policy and strategy document should be directed to the Risk Management Unit (RMU) within the Corporate Governance Directorate.
- d) The RMU is available to offer advice and assistance on risk management / internal control issues.



Tshediso Matona
DIRECTOR GENERAL: the dti
DATE: 10/03/2008



Appendix A

ANTI-FRAUD CHARTER

In implementing the Fraud Policy of the Department of Trade and Industry:

We have a zero-tolerance attitude to fraud and corruption

- We are instituting and maintaining an anti-fraud environment throughout the Department.
- The fraud prevention plan is being implemented throughout the Department.
- Fraud reduction is a priority in both divisions and agencies of the Department.
- We will embrace and acknowledge the contribution of all employees and members of the community who assist in the combating of fraud and in the prosecution of fraudsters.

We understand and manage our risks

- Our fraud and corruption risks are reviewed and assessed on a regular basis.
- Cognisance to fraud risks is given in all procedural changes.
- Internal controls and audit measures are in place to identify and manage fraud risk.

We are proactive in defending our assets

- We pursue strategic alliances in combating fraud.
- We are establishing a profile on potential fraudsters.
- We are monitoring direct and indirect losses incurred via fraud, through effective information and communication.

We react swiftly when a crime is uncovered

- We react swiftly and appropriately when a crime is uncovered.

In ensuring that this commitment is shared by all employees, this Charter shall be signed by every staff member of the dti.

The accounting officer, on behalf of the dti employees by virtue of his signature reflected below, hereby subscribes to the terms of this Charter.

Tshediso Matona
DIRECTOR GENERAL: the dti
DATE: 10/03/2010

APPENDIX B: FRAUD PREVENTION MATRIX / IMPLEMENTATION DELIVERABLES

FPP Matrix of Tasks and Responsibilities

Based on RMC FPP for 2009/10

TASK	RESPONSIBLE PERSON	TARGET DATE	EFFECTIVE DATE	PROGRESS
EMBEDDING AN ETHICAL CULTURE				
Develop an Ethics Framework	RMO and HR	Q2	July 2009	
Ensure all employees confirm their understanding of the Ethics Framework				
Conduct workshops on Promotion of Ethical behaviour	RMO	Q3	September 2009	
Monitor Ethical behaviour by way of surveys/questionnaires and interviews where necessary	RMO	Q3	September 2009	
FRAUD AWARENESS TRAINING				
Conduct fraud awareness and training to newly appointed staff at induction	RMO	Annually	Every Induction session	
Conduct fraud awareness and training to all staff	RMO	Q2	August 2009	
FRAUD RISK MANAGEMENT				
Conduct fraud risks assessments	RMO	Every 12-18 months	Q4	
Monitor fraud risks	Risk Champions	Monthly	Monthly	
INTERNAL CONTROL				
Regular communication of the policy and conduct awareness campaigns	Marketing/RMO	Monthly	Monthly	
PRE-EMPLOYMENT SCREENING				
Pre-employment screening	HR	As and when candidates are appointed	As and when candidates are appointed	
Security Vetting	AMS			
DISCLOSURE OF INTERESTS				
Disclosure of Financial Interests (All staff)	RMO/ Risk Champions	Annually	As and when there is a need to disclose	
Monitor and Examine Financial Disclosures	RMO/IA	Annually	Annually	
DETECTION				
Management Reporting Review	Finance			
Identification of early warning signs	IA			
Reporting instances of fraud(Whistleblowing)	IA			
PHYSICAL SECURITY				
Monitoring Access in the campus	AMS			