DEPARTMENT OF COMMUNITY SAFETY AND LIAISON

FRAUD PREVENTION POLICY

CONTENTS

FRAUD POLICY STATEMENT

I, Head of the Department of Community Safety and Liaison, representing and acting on behalf of the communities of the Province recognise that fraud undermines our vision and mission against crime.

As a Department, it is important that we live out these values everyday and act against activities that are not aligned with our norms.

I hereby irrevocably commit this Department to a Zero Tolerance Approach to fraud in all its forms. Parties found to be in violation of this policy will be prosecuted.

Signed, this 3rd day of February 2014, by

Acting Head of Department: Community Safety and Liaison

FRAUD PREVENTION POLICY

1. BACKGROUND

1.1. This policy sets out the stance of the Department to fraud and corruption as well as to reinforcing existing systems, policies, procedures, rules and regulations of the Department aimed at deterring, preventing, detecting, reacting to and reducing the impact of fraud.

1.2. Furthermore, the purpose and spirit of this document is to confirm that the Department supports and fosters a culture of zero tolerance to fraud and corruption in all its manifestations.

1.3. The Department recognises that acts of fraud by its employees seriously deplete the scarce resources available to the Department in fulfilling its mandate.

1.4. The Department also recognises that the debilitating effects of fraud extends beyond the loss of cash and other assets which have severe negative repercussions on the ability of Department of Community Safety and Liaison to achieve its objectives. Although difficult to quantify, such acts, if left unchecked, seriously reduce:

(a) The quality and effectiveness of service delivery;
(b) The strength of business relationships with clients, suppliers and the public;
(c) Employee morale; and
(d) The reputation and image of Department of Community Safety and Liaison.

2. SCOPE OF THE POLICY

Persons to whom the policy applies

2.1. This policy applies to all employees of Department of Community Safety and Liaison and relates to all attempts and incidents of commercial crimes, including fraud, impacting or having the potential to impact on Department of Community Safety and Liaison.

3. POLICY DEFINITIONS

"Commercial crimes" Crimes that cause actual and/or potential losses when committed and include fraud, theft and corruption.

Actions constituting commercial crimes

Actions constituting commercial crimes may include, but are not limited to, the following:

(a) Any dishonest or corrupt act;
(b) Theft of funds, supplies or other assets;
(c) Maladministration or financial misconduct in handling or reporting of money, financial transactions or other assets;
(d) Making a profit from insider knowledge;
(e) Disclosing confidential or proprietary information to outside parties for financial or other advantage;
(f) Requesting or accepting anything of material value (free of charge) from contractors, suppliers or other persons providing goods or services to Department of Community Safety and Liaison;
(g) Irregular destruction, removal or abuse of records and equipment;
(h) Deliberately omitting or refusing to report or act upon reports of any such irregular or dishonest conduct;
(i) Bribery, blackmail, secret commissions and or extortion involving the Department employee in the performance of her or his duties;
(j) Abuse of the Department's facilities; and
(k) Any similar or related irregularity.

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

"Department" Department of Community Safety and Liaison

"Fraud"	The unlawful and intentional making of a misrepresentation resulting in actual or potential prejudice to another party.
"ICRMU"	Departmental Internal Control and Risk Management Unit
"IAU"	Internal Audit Unit of the Provincial Treasury
"Theft"	The unlawful and intentional misappropriation of another's property or property which is in his/her lawful possession, with the intention to deprive the owner of its rights permanently.

4. STATEMENT OF OVERALL POLICY

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

4.2. It is the responsibility of all employees of Department of Community Safety and Liaison to report all incidents of fraud to her/his Manager/Head of Department.

4.3. All employees within Department of Community Safety and Liaison are responsible for the prevention and detection of fraud.

4.4. All Managers shall regularly cause their systems to be reviewed for resilience against commercial crime (including fraud) and ensure that appropriate changes are made to ensure that systems are fraud resistant.

4.5. The Head of Department and respective Managers are required to ensure that losses or damages suffered by Department of Community Safety and Liaison as a result of all reported acts of

commercial crimes committed or omitted by an employee or any other person, are recovered from such an employee or other person if he or she is found to be liable.

5. CONFIDENTIALITY

5.1. All information relating to commercial crimes received and investigated will be treated confidentially. The progression of investigations will be handled in a confidential manner and will not be disclosed or discussed with any person(s) other than those who have a legitimate right to such information. This is important to avoid harming the reputations of suspected persons who are subsequently found innocent of wrongful conduct.

5.2. No person is authorised to supply any information with regard to allegations or incidents of fraud to the media without the express permission of the Head of Department.

6. PUBLICATION OF SANCTIONS

6.1. The Head of Department will decide, in consultation with appropriate Senior Managers, whether any information relating to corrective actions taken or sanctions imposed regarding incidents of fraud should be brought to the direct attention of any person or made public through any means.

7. PROTECTION OF WHISTLE BLOWERS

7.1. No person will suffer any penalty or retribution for reporting in good faith, any suspected or actual incident of commercial crimes.

7.2. Managers should discourage employees or other parties from making allegations, which are false and made with malicious intentions. Where such allegations are discovered, the person who reported the false allegation will be subjected to firm disciplinary or other appropriate action.

8. ADMINISTRATION

8.1. The custodian of this policy is the Head of Department who is supported in its implementation by all Managers within the Department of Community Safety and Liaison.

8.2. The ICRMU, supported by the Head of Department and all Managers of Department of Community Safety and Liaison, is responsible for the administration and revision of this policy. This policy will be reviewed annually and appropriate changes will be made should these be required.

FRAUD PREVENTION RESPONSE PLAN

1. APPLICATION OF PREVENTION CONTROLS AND DETECTION MECHANISMS

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

1.2. Ongoing risk assessments will be conducted to identify risks and implement effective and efficient internal control systems.

1.3. The Department has a number of systems, policies, procedures, rules and regulations designed to ensure compliance with prevailing legislation and to limit risk, including the risks of fraud. Fundamentally, all employees of the Department should understand and must comply with these.

1.4. The following are some of the relevant policies, procedures, rules and regulations:

(a) Public Finance Management Act as amended;
(b) National Treasury Regulations;
(c) Departmental Policies;
(d) National and Provincial Practice Notes;
(e) Departmental Disciplinary Code and Procedures;
(f) Procurement Delegations
(g) Code of Conduct for Public Servants;
(h) Conditions of Service and Human Resources Policies and Procedures detailed in the Public Service Regulations; and
(i) Delegations of Authority

1.5. Internal audits and ad-hoc procedures will be undertaken to monitor and evaluate the extent of compliance with policies and procedures. In instances where serious breaches occur, swift and efficient disciplinary action will be considered to set an example to other potential wrongdoers.

1.6. New policies and procedures and strategic plans will be circulated to staff at appropriate levels, in draft format, for the input and comments before these are finalised.

1.7. The system for pre-employment screening of candidates shall ensure that the best candidates are employed.

1.8. A specific effort will be made to ensure that the guidelines issued by National and KZN Provincial Treasury, for the placing of restrictions on suppliers and/or other providers of goods and/or services who are found guilty of unethical conduct or other irregularities, are pursued vehemently. Any employee found to be colluding with suppliers will be subjected to immediate disciplinary action and any losses suffered by the Department will be recouped from the employee.

1.9. Internal Controls

1.9.1 Prevention controls

Authorisation:

(a) All transactions require authorisation or approval by a responsible person with appropriate authority limits.
(b) The authority limits are specified in the delegations of authority of the Department.

Physical:

All assets shall be:
(a) Assigned to persons responsible for safeguarding the assets.
(b) Adequately safeguarded by the persons responsible for the assets.

1.9.2 Detection controls shall include at least:

Arithmetic and accounting:

(a) These are basic controls within the recording function that check that transactions to be recorded and processed have been authorised and that they are

completely and correctly recorded and accurately processed.

(b) Such controls include checking the arithmetical accuracy of the records, the maintenance and checking of totals, reconciliation and accounting for documents.

Physical:

(a) These controls relate to the security of records. They therefore underpin arithmetic and accounting controls.
(b) Their similarity to preventive controls lies in the fact that these controls are also designed to limit access to unauthorised persons.

Supervision:

This control relates to supervision by Managers of day-to-day transactions and the recording thereof.

Management information:

(a) This relates to the review of management accounts and budgetary control.
(b) These controls are normally exercised by management outside the day-to-day routine of the system.

1.9.3 Division of duties

The lack of division of duties or the overriding of existing internal controls is a generic risk that exposes the Department to the inherent risk of fraud and manipulation of data. One of the primary means of control is the separation of those responsibilities or duties, which, if combined, enable one individual to record and process a complete transaction, thereby providing him/her with the opportunity to manipulate the transaction irregularly and commit fraud.

Division of duties reduces the risk of intentional manipulation or error and increases the element of checking.

All employees within the Department 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 Managers to the Head of Department or alternatively to the ICRMU.

1.9.4 Physical security

(a) Recognising that effective physical security is one of the "front line" defences against fraud, the Department will take regular steps to improve physical security and access control at its offices in order to limit the risk of theft of assets;

(b) The Department shall also regularly review the physical security arrangements at its offices and improve on weaknesses identified.

1.9.5 Information security

(a) The Department acknowledges the key risks of fraud in this area as the following:

(i) Risk of disclosure of confidential information;

(ii) Manipulation of data without appropriate authorisation procedures through inappropriate access to information.

(b) The Department will ensure that employees are sensitised on a regular basis to the risks of fraud associated with poor management of information security in order to enhance their understanding thereof and the risks to the Department associated with poor control over confidential information.

(c) Regular reviews of information and information technology security will be carried out. Weaknesses identified during these reviews will be addressed with the respective Managers.

(d) In respect of information technology, regular communiques will be forwarded to employees pointing out the content of the IT Policy and procedures, with particular emphasis on internet and email usage and the implications (eg. disciplinary action) of abusing

these and other computer-related facilities. Where employees are found to have infringed on prevailing policy in this regard, disciplinary action will be taken.

2. WHISTLE BLOWING POLICY

2.1. In order to further limit the risk of employees being victimised for whistle blowing, in contravention of the Protected Disclosures Act (2000), the Department has developed a Whistle Blowing Policy attached to this plan.

2.2. The Whistle Blowing Policy is based on the Protective Disclosures Act (2000), which guarantees protection to employees against victimisation following disclosure of fraudulent activity by employees, and is intended to encourage and enable employees to raise serious concerns without fear of victimisation.

2.3. The Whistle Blowing Policy, which is attached as an addendum to the Fraud Prevention Policy, will be circulated to all employees within the Department.

3. FORENSIC INVESTIGATIONS

3.1. Any reported case requiring forensic investigation will be referred to the Internal Audit Unit for investigation.

3.2. It is the responsibility of the Head of Department to implement the recommendations made in the forensic report.

4. REPORTING PROCEDURES AND RESOLUTION OF REPORTED INCIDENTS

4.1. What should employees do when commercial crimes (including fraud) are suspected?

(a) Any employee who suspects commercial crime (including fraud) shall immediately report all allegations or incidents of

commercial crimes to their immediate Manager or, if the employee has reason to believe that his/her immediate Manager is involved, to the next level of management. All Managers must report all incidents and allegations of commercial crimes to the Head of Department, CFO or the ICRMU.

(b) The Head of Department shall then communicate the allegation to the relevant component or to the ICRMU for investigation.

(c) Should employees wish to report allegations of fraud anonymously, they can contact any member of management, the Head of Department, the ICRMU or the IAU of Provincial Treasury (PO Box 3613, Pietermaritzburg, 3200).

(d) Suspected fraudulent activities can also be reported on the following hotlines:

- Presidential Hotline (17737)
- KZN Operation Sukuma Sakhe Hotline (0800 596 596)
- National Anti-Corruption Hotline (0800 701 701)

4.2. What should a member of the public do if they suspect fraud impacting the Department?

The Department encourages members of the public who suspect fraud to contact the Head of Department, the ICRMU, the IAU or phone the hotline/s as listed above.

4.3. How will allegations of fraud be dealt with by the Department?

(a) The Head of Department or his/her delegated representative will, upon receiving a report of fraud from an external person, write to the person (unless the report has been made anonymously) making the report:

(i) Acknowledging that the concern has been received; and

(ii) Informing her or him whether any further investigations will take place, and if not, why not.

(b) The Department accepts that those people, including employees who reported the alleged fraud need to be assured that the matter has been properly addressed. Thus, subject to legal constraints, information about outcomes of any investigation will be disseminated on a "need to know" basis.

(c) The action taken by the Department will depend on the nature of the concern and will be pursued by thorough investigation and to the full extent of the law. The matters raised may be investigated by the ICRMU or the IAU and/or referred to the SAPS. Where misconduct or commercial crime is found, the investigation's objectives will include disciplinary actions and institute of criminal proceedings.

(d) The Departmental Internal Control and Risk Management Compliance Committee will regularly review the matters reported and actions taken.

5. CREATING AWARENESS

5.1. It is the responsibility of all SMS Members to ensure that all employees under their area of responsibility are made aware of this policy.

5.2. The ICRMU is responsible for communicating relevant sections of this policy to members of the public or other stakeholders of Department of Community Safety and Liaison.

6. ADDENDUM

The following documents form part of the Fraud Prevention Policy:

Annexure A: Whistle Blowing Policy
Annexure B: Explanatory Manual on the Code of Conduct

Annexure C:	Provincial Policy on the acceptance of gifts, rewards, awards, sponsorships, donations, and hospitality by employees
Annexure D:	Gift Register