JOHANNEBURG CITY PARKS AND ZOO

FRAUD PREVENTION BOOKLET

This booklet seeks to educate all JCPZ stakeholder i.e. employees, suppliers/service providers and members of the public on the issues of fraud and corruption. It also informs the stakeholders on JCPZ stance towards fraud and corruption.

TABLE OF CONTENTS

1. INTRODUCTION

The purpose of this booklet is to provide JCPZ employees (both management and staff) and other stakeholders (such as the public, service providers and contractors) with some essential information regarding the fraud & corruption and whistleblowing policies as well as responsibilities of the various role players in combating corruption.

A centralised Tip off Line has been established by the City of Johannesburg (CoJ) and operational to enable all to report any fraud and/or corruption activities. It is the Internal Audit intent to regularly embark on fraud prevention programmes in order to ensure that fraud and corruption activities are reduced and stakeholders are discouraged from being engaged into any fraudulent activities.

2. DEFINITIONS

2.1 CORRUPTION

An act of 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

2.2 DEFINITION OF FRAUD

"the unlawful and intentional making of a misrepresentation resulting in actual or potential prejudice to another"

3. THE NATURE OF FRAUD

There are a number of elements which are common in many instances of fraud.

For example:

- Most frauds involve employees or management and many others are committed in collusion with outsiders.

- Both major and minor frauds can be highly sophisticated or very simple. Employees often take advantage of weaknesses in controls which they become aware of during the course of their daily work.

- There are many motives for fraud. Some of the most common include personal financial problems, greed, grudges or the need to fund gambling or drug addiction.

4. FRAUDULENT AND CORRUPT ACTS

Fraudulent and corrupt acts may include the following:

***Systems Issues*:** where a process/system exists which is prone to abuse by either employees or the public, e.g.:

- Maladministration or financial misconduct in handling or reporting of money, financial transactions or other assets;
- Disclosing confidential or proprietary information to outside parties;
- Procurement fraud e.g. irregular collusion in awarding of tenders or orders for good and/or services; and
- Deliberate non-compliance with delegation of authority limits.

***Financial Issues*:** i.e. where individuals or companies have fraudulently obtained money from the company, e.g.

- Creditors fraud e.g. diverting payments to incorrect creditors;
- Irregular collusion in awarding contracts or orders for goods and/or services;
- Suppliers submitting invalid invoices or invoicing for work not done;
- Payroll fraud e.g. creation of ghost employees;
- Revenue fraud e.g. irregular refunds to consumers; and
- Theft of funds;

***Equipment and Resource Issues*:** i.e., where the company's equipment is utilised for personal benefit, e.g.:

- Unauthorised use of company resources for personal benefit. vehicles of the company;
- Theft of assets e.g. printer cartridges; and
- Irregular destruction, removal, or abuse of records (including intellectual property) and equipment;

***Other Issues*:** i.e., activities undertaken by officers of the company which may be unlawful against the company's regulations or policies, falls below established standards or practices or amounts to improper conduct, e.g.:

- Soliciting , Accepting and/or Receiving undue gifts or favours for rendering services, e.g. expensive gifts in contradiction of the Code;
- Conflict of interest;
- Nepotism and/or favouritism and
- Deliberately omitting or refusing to report or act upon reports of any such irregular or dishonest conduct.

5. FRAUD INDICATORS - RED FLAGS OF FRAUD AND CORRUPTION

- Fraud indicators are best described as clues or hints that a closer look should be made at an area or activity.
- The term "red flag" refers to anomalies, unusual events, a signal that informs or indicates, announces or communicates that something is different from the norm or the expected activity.
- Identifying red flags is very crucial for the process of fraud detection. (Refer Annexure A for general indicators and common indicators for high risk areas)

GENERAL RED FLAGS

- **Weak ethical practices**. Senior management sets a poor example for employees to emulate. A code of ethics policy may not exist.
- The employees don't take leave or no long vacations and are posted on the same position for more than the normal tenure time.
- **Inadequate review process**. If there is inadequate review processes the likelihood of an increase in irregularities and fraud increases.

- **Approval fails to meet standard or normal approval processes.** Exceptions to approval processes should be reviewed to determine why these were processed differently.

- **Non-compliance with authorities.** Entity does not comply with government acts and statutory regulations.

- **Conflicting evidence.** When supporting documentation is in conflict with management's or employees' response to inquiries, the transaction should be considered suspicious.

- **Internal controls that are not enforced or are overridden by management**.
  When management frequently overrides key internal controls or does not enforce the controls, this may suggest a pattern that indicates possible wrongdoing and fraud.

- **Information is provided to the auditor unwillingly or following unreasonable delays. Failure to respond to information requests in a timely manner** raises suspicion about the integrity of the transaction; delays could enable the perpetrators to create fictitious documentation to support the **requested transactions.**

- **Missing documentation. The absence of invoices, delivery receipts or consultants' products may indicate that a payment** was made for goods that had not been received or services that had not been provided. Missing signed approval forms for invoices, contracts, or grants and contribution awards may indicate that appropriate approvals had not been obtained.

- **Only photocopies**, **faxes or scanned documents are available**. Auditors should review original documentation for proper examination. If only photocopies, faxes or scanned documents are available, this could indicate that originals do not exist or portions of original documents are being hidden from management or auditors or original documents were altered through the photocopying, faxing or scanning process.
- **Alterations and discrepancies in documentation.** Documents should be **considered suspicious when an addition, deletion** or variation has been made to the original content. Alterations may include erasures, opaque or obliterated entries, the addition of new last letters or numbers, the distortion of patches over existing content. In the case of typed or printed text, changes may include adding or deleting sections after the original document has been approved and signed. Payment information that is different from the supporting documentation, for example a new amount or a different name of the payee, should raise questions with the auditor.

- **Bogus documents or fictitious invoices.** When a document's origin cannot be identified or it contains suspicious content, it is most likely fraudulent. Signs of fraud may include using more than one typewriting style, font or typeface, and inconsistent spacing of data. Invoices that do not contain a street address, postal code or telephone number are questionable and need to be investigated.
  An invoice with only a post office box number for an address or without a goods and services tax registration number and tax amounts may indicate fraud.

- **Hand-written documents are provided instead of computerized documents.** In cases where one would normally expect to find a computerized document, a hand-written document may indicate a fictitious document.

- **Incorrect or revised versions of key documents**. Auditors should ensure they have the final version of contracts and agreements to ensure a proper review. They must also watch out for substituted or missing pages in long documents.

- **Fictitious contractor or supplier.** Invoices from a company with a name that is similar to a legitimate vendor name may be fictitious.

- **Transactions that are not processed through the normal accounting process.** Failure to follow normal accounting processes should be looked at to determine why these transactions have been processed differently. Such practices could suggest a pattern of irregularities.

- **Transactions not recorded in a complete or timely manner**. Transactions that are not completed in a timely manner or are improperly recorded as to classification or accounting period may indicate irregularities.

- **Odd**, **unusual or different transactions**. Transactions that do not make sense or are out of the ordinary need to be examined thoroughly by the auditor. Transactions that are peculiar in the time of day or week, in frequency (too many or too few), in place (too far or too near) or in amount (too high, too low, too consistent or too different) may be suspect.

6. COMMONLY FOUND FRAUDS IN MAJOR AREAS.

Contracts (Procurement, Service and Construction)

The following are common methods of perpetrating contract fraud,

- **Bribery and kickbacks—**a contractor gives government employee money, gifts, or other favours in order to obtain business or favourable treatment.

- **Change order abuse—**changes are made to the original contract conditions, resulting in a need for more funds than were provided in the original contract. Change orders may be issued throughout the life of the contract to compensate contractor who initially submitted a low bid.

- **Collusive bidding, price fixing, or bid-rigging—**a group of prospective contractors may make an arrange**ment to eliminate o**r limit competition

- **Co-mingling of contracts—**a contr**actor bills for th**e same work under more than one contract.

- **Conflict of interest—**contracts are awarded to organizations that employ government employees or their families, or to companies in which government employees or their families have an undisclosed financial interest.

- **Defective pricing**—a contractor submits inflated invoices that do not comply with the costs/prices specified in the contract.

- **Duplicate invoices—**a contractor submits separately two copies of the same invoice and is subsequently paid twice.

- **False invoices—**a contractor submits invoices for goods that have not been delivered, or the invoice does not reflect the contract terms.

- **False quality and performance representations**—a contractor makes false representations about the quality of the products to be supplied or qualifications to perform the requested services.

- **Information disclosure—**a government employee releases unauthorized information to a contractor to assist that contractor to win the contract

- **Local purchase order abuse or split purchases**—the total cost of purchasing goods and services exceeds the local authority limit, or a competitive process is required to provide such goods or services. To bypass these rules, the purchases are split into two or more segments.

- **Phantom contractor**— a contractor submits an invoice from a nonexistent company to support fictitious costs contained in a government cost-plus contract.

- **Product substitution**—a contractor fails to deliver the goods or services as specified in the contract. The contractor may substitute an inferior product without informing the government.

- **Progress payment abuse: front-end loading or advance payment**— under government contracts, payments are made as work progresses. The payments are based on the costs incurred, the percentage of work completed, or the completion of particular stages of work. Progress payment fraud normally includes falsified certification of the work completed in order to receive payments prior to the work being done. The contractor may inflate the costs of the initial work so that, when the percentage of completion billing method is applied; the contractor would receive higher cash flows relative to the actual
  work completed. The cost of subsequent contract work would be understated with the anticipation that change orders would be approved for additional compensation.

- **Purchases for personal use**— a government official purchases items for personal use, or makes excess purchases of which some items are diverted for personal use.

- **Short bidding time limits—**the lead-time for responding to a proposal is unusually short so that only bidders with inside knowledge will be able to prepare a proposal on time. There is no compelling reason to justify a markedly reduced response time.

- **Tailored specifications—**a government official establishes unnecessary or highly restrictive product specifications that only one contractor can meet.

- **Unnecessary purchases—**goods or services that have been previously purchased are purchased again when there is no additional need.

Revenue collection

The following are the frauds commonly found in the area of revenue collection.

- **False disclosure**—an organization makes false disclosures to the government to maximize its profits. The organization submits false information on the quantity and quality of the resources to minimize the taxes it must pay. The organization submits false information concerning the revenues earned from its commercial application

- **Theft of revenue receivable**—an employee steals a payment of revenue received. Or an employee enters only part of the payment of revenue received in the accounting records and pockets the difference. To avoid being detected, the employee posts B's payment to A's account, C's payment to B's account, etc. This process, called lapping, requires continuous manipulation and monitoring of many accounts and transactions.
- **Revenue receivable write-offs**—an employee writes off as uncollectible, revenue receivable that are not really in arrears or will likely be collected. This is done to conceal the theft of accounts receivable payments or the future theft of payments.

- **Bribery or kickbacks**—an individual gives a government employee money or gifts in order to receive preferential treatment. For example, an individual gives money to a government employee to obtain surplus Government assets at a low price.

- **Conflict of interest**—a government employee has an undisclosed personal interest that may affect, or be perceived to affect, his/her independence and objectivity in carrying out his/her job responsibilities. In the context of revenues, a government official sells goods or services to a company that employs his/her spouse at lower prices or collects less revenue from an industry on favourable terms than those that could have been negotiated with another company.

- **Disposal of assets for personal gain**—a government employee with a personal interest in government assets could identify those assets as surplus goods even though they still have a government purpose. The sole reason the employee identifies those assets as surplus is to purchase them for personal benefit.

- **Information theft**—a government employee releases information to a third party without charge when the information should have been sold.

Asset management (Cash & Inventory)

The types of assets frauds include:

- **Employees take assets for personal use**—an employee misappropriates an organization's assets for his/her personal use without attempting to conceal the theft in the organizations books. Or, an employee sells assets for cash without recording the disposal.

- **Assets are sold at less than fair market value**—assets are sold or disposed of at less than fair market value to someone related to an employee. Or, asset disposal may be recorded at a value less than what was received, and the employee misappropriates the difference.

- **Asset requisitions and other documents are used to move assets to another location to facilitate theft**—an employee overstates the amount of supplies and materials needed for a project and takes the excess. Or, false shipping documents are used to ship assets to the employee or to an accomplice.

- **Purchasing and receiving functions are manipulated**—an employee receiving goods on behalf of the organization falsifies incoming shipments and takes part of the shipment.

- **Shipment of excessive quantities to a third party, who then declares bankruptcy**. This is common fraud found in the area of asset management.

- **Large unexplained inventory shortage**, particularly of inventory that has resale value. This is a symptom of employee theft of assets.

- **Non Existent inventory pledged as collateral**

Program management

- **Conflict of interest—**having undeclared private interests that could affect, or be perceived to affect, the independence and objectivity of an individual in carrying out official duties. For example, a government official recommends that a program be funded by the government where his relatives be in the management.

- **Embezzlement—**taking money that has been lawfully received and using it, without the knowledge and consent of the provider of the funds, for other purposes.

- **False representation**—knowingly making false or misleading statements to gain an improper advantage. In the context of program management, this could involve making false statements to mislead the government in order to obtain funding.

- **Fraudulent concealment**—knowingly hiding information that is necessary and important to the funding decision and program monitoring.

- **Improper or unusual approval authorities**—those approving funding applications do not have the require delegated authority. Or senior officials, who would not normally be involved in the approval process, take a special interest in the approval of the funding application of a program and its subsequent management.

- **Questionable or fraudulent performance reporting—**a funding recipient does not submit all the performance information required by the agreement Or the quality and completeness of the performance is so poor that there are suspicions about how funds were used. Minimum or no performance information may indicate that government funds were diverted to other unauthorized projects or used for personal benefit.

General expenditure (Payroll, expense and credit cards)

The commonly found frauds in Payroll accounts are:

- **Overtime abuse**—employees are responsible for approving their own overtime without supervisory oversight. Sometimes supervisors and employees collude in overtime abuse by splitting the overtime payments.

- **Overpayment**—an employee is paid at a higher rate of pay than he/she is entitled to and does not disclose the errors.

- **Annual leave cash out**—an employee cashes out his/her annual leave, even though he/she took leave throughout the year but did not submit leave notices.

- **Severance pay**—an employee receives severance pay even though he/she is still working for a department, or is ineligible.

- **Ghost employees**—a fictitious employee is put on a department's payroll, and payments for that employee are deposited into the perpetrator's bank account or the account of one of his/her family members. With electronic payroll deposits, it is more difficult to uncover ghost employees.

- **Terminated employees are not deleted from the payroll system**
  Payments continue to be made to terminated or retired employees, those who have resigned, or those who are on medical leave. Payroll payments are deposited into the perpetrator's bank account or the account of one of his/her family members.

- **Employment insurance fraud**—false records of employment are issued to an employee so that he/she can meet the eligibility requirements of the employment insurance program.

- **Staffing and classification abuse**—managers who are behaving inappropriately may gain the cooperation of their staff by reclassifying positions to higher salary levels or changing casual or term positions indeterminate positions.

- **Personal expenses are submitted as business expenditures.** An employee submits personal expenses such as computer accessories, automobile fuel purchases, or personal meals as business expenses.

- **Expenses are submitted twice.** An employee is reimbursed more than once for the same expenses or items that have been purchased and paid for by the entity, and also claimed in an expense report or claim. For example, the government may prepay an expense such as an airline ticket. The ticket is changed and a new ticket is issued for a nominal charge; the employee submits the total charges of the revised airline ticket for reimbursement.

- **A claim for expenses that someone else paid for is submitted for reimbursement.** For example, three government employees share a taxi and all three submit the taxi fare on their expense reports. Or, a meal already paid for under a hospitality expense or conference is subsequently claimed by an employee as part of his/her daily meal allowance.

- **A false claim for automobile kilometre charges is submitted.** An employee submits a claim for automobile kilometres that is higher than the actual kilometres driven.

- **An invoice is submitted for an item that was returned for a refund.** For example, an employee submits a copy of the purchase invoice for a computer accessory, when a refund for the item was subsequently received.

- For credit cards the following are the commonly found frauds,

- **Personal purchases**—a government employee cardholder purchases goods or services for personal use on their government credit card, without authority to do so, and allows the department or agency to pay for these goods or services without reimbursing the employer. This fraud can go undetected if the goods and services appear to be normal government purchases such as computers, automobile fuel, and travel and hospitality expenses.

- **Unauthorized billings**—an individual who, intentionally and without the cardholder's knowledge, permits the billing of personal or nongovernment items on a government credit card and does not reimburse the government for these purchases. This fraud is often undetected if the government cardholder does not verify all charges on the credit card statement before authorizing the payment of the outstanding balance.

- **Unauthorized charges by retailers, wholesalers, and contractors**—in this kind of fraud, businesses will process charges against government credit cards for goods and services that were never authorized or never provided. This kind of fraud also includes inflating charges on government credit cards that do not reflect the agreed upon amount for the goods and services provided. This fraud goe**s undetected if the government cardholder does not verify all c**harges on the government credit card statement against invoices or purchase orders and permits the outstanding credit card balance to be paid.

IT Environment

The frauds committed in IT environment are:

- **Altering or falsifying computer input** transactions to conceal problems **such as misappropriation of funds or** assets;

- **Implementing computer program changes for personal gain** e.g. an employee manipulating systems to have payments made to himself/ herself

- **Stealing computer data** and selling it to third parties;

- **Direct computer file changes** by an employee for his/her benefit;

- **Transferring funds electronically** and subsequently destroying the audit trail; and inappropriately accessing computer information that can be used to commit an illegal activity (e.g. a person hacks into a government computer server and views confidential information that will be publicly announced shortly which will impact on share values of certain publicly traded companies and uses this confidential information to make gains on the stock market.

  Commonly found internet frauds include**;**

- **Theft of funds through false Government Online applications**;

- **Identity theft** or using such stolen identity through the Internet;

- **Illegal use of government credit card numbers** for purchases on the Internet;

- **Selling on the Internet**, products or services that do not exist;

- **Stealing data via the Internet** for personal benefit or selling it to third parties;

- **Sabotaging computer systems**, including planting viruses and worms by hacking into computer systems via the Internet, which affects network downtime and destroys valuable computer information;

- **Sending endless SPAM** to government Web sites

7. JCP TIP-OFF ANONYMOUS HOTLINE 

The City of Johannesburg has established a centralised **anonymous** tip off line for all its entities in order for employees and other stakeholders to freely report concerns without any fears of victimisation. The hotline is independently managed by external service provider. The TOA became operational on October 2012.

The toll free number for the hotline is **0800 002 587**. It is established to achieve the following:

- To encourage employees and other stakeholders to report any fraudulent activities that they witness or which come to their attention without any fear of victimization
- To assist JCPZ to identify areas of fraud risk so that preventive and detective controls can be improved.
- To raise the level of awareness that JCPZ is serious about fraud and corruption

Receiving and processing of tip-offs

- Calls are answered live 24 hours a day, seven days a week, and 365 days per year.
- Currently, it offers a number of language choices, including English, Afrikaans, isiZulu and isiXhosa language. For the most of each day, other languages such as isiNdebele, Sepedi, Sesotho, Setswana, siSwati, Tshivenda, Xitsonga and Portuguese languages are also offered.
- Response to callers will be customised. Deloitte Personnel have the ability to ask specific questions about the incident in order to obtain more information to enable effective investigation of the allegation. .
- Tip-offs are then assessed by trained report analysts, some of which are experienced ex SAPS Commercial Branch detectives, for urgency and importance. They are also summarised and sanitised to ensure the caller remains anonymous.
- Tip-off reports will attempt to indicate the nature of the tip-off (for example - abuse of assets, theft, invalid payments, etc) for easy reference and classification.

7. Deloitte.

FREECALL: 0800 002 587

Or

Email : anticorruption@tip-offs.com

Generic Questions & Prompts

Generic questions and prompts to expect when calling the Tip Off Line

1. *When did the irregularity occur?*
2. *What do you know/what did you witness?*
3. *With regards to the incident:*
    - *Do you know the people involved?*
    - *Registration of fleet vehicle(s) involved/where do they work?*
    - *Is this the first time, if not when did this start?*
    - *Is it still happening?*
    - *Did anyone see what took place?*
    - *Have you reported the incident to anyone else in your organization or to senior /supervisor?*
    - *Do you have any proof? (Can you send it to)?*
    - *Was the money or any favours exchanged?*
    - *When did this take place (date and time)?*

Supplier

5. *Which supplier or contractor are you with?*

6. *Which delivery site/project did the irregularity take place at, and when did it happen?*

7. *Which projects are u involved in?*

8. *With regards to the incident:*

- *Name of people involved;*
- *Registration of fleet vehicles involved*
- *How long has this been going on?*
- *Is it still happening?*
- *Who else knows about it?*
- *Have you reported the incident to anyone else in your organization*
- *Do you have any proof? (Can you send it to TOA)?*
- *Is there any exchange of money, and how much?*
- *Are there any witnesses?*

9. FEQUENTLY ASKED QUESTIONS 

Will feedback be provided to employees?

Tracing / reference number will be provided to get feedback from the call centre.

Are there any benefits to be derived from reporting other employees on the Tip Off Anonymous (TOA) Line?

Not only will employees be saving their jobs by reporting but also the company they work for, as, if unethical behaviour continues and the company keeps losing money, it will have to retrench employees, salary increases and promotions withheld and so forth.

Are employees able to report historical events?

Tip-offs is able to assist with the reporting historical allegation but we encourage reporting these allegation only if there is proof or they can still be proven.

How will TOA guarantee employees protection? For example if someone report an employee and that employee find out they have been reported, how will they be protected from intimidation.

Identity remains unknown

If the calls are being recorded then it means they are able to trace the voices to that particular employee?

The recordings remain Deloitte's property, and cannot be shared with the client, in this case, JCPZ.

How does TOA deal with false allegations?

An investigative process will take place to probe the validity of the allegation. Tip offs will also vet the allegation prior and if we believe this to be a malicious allegation, it will state as such on the tip-off report.

Is this targeted at employees only, or can they also report any misconduct by the general public

The public can also be reported provided that employee's have evidence or proof of the allegations.

10. LEGAL FRAMEWORK 

The following legislation and policies, amongst others, deal with fraud and corruption in South Africa:

- The Constitution of the Republic of South Africa ,1996
- Local Government: Municipal Systems Act, Act 32 of 2000
- Municipal Finance Management Act, Act No 56 of 2004
- Prevention of Organised Crime Act, 121 of 1998
- Prevention and Combating of Corrupt Activities Act, Act 2004
- Corruption Act, Act 94 of 1992
- Treasury Regulations
- Protected Disclosures Act, Act 26 of 2000
- JCPZ Code of conduct
- Anti- Corruption and Whistle-blowing policies (JCPZ)

In view of the legal framework and policies, Johannesburg City Parks and Zoo is committed to creating an environment that is based on the prevention of fraud and corruption. This is achieved by promoting a culture of openness and honesty in all its activities.

11. APPENDIX

11.1 JCP ANTI FRAUD & CORRUPTION POLICY

POLICY STATEMENT

Johannesburg City Parks and Zoo adopts a culture of “zero tolerance” to fraud and corruption.

Staff are forbidden to participate in any activity of fraud and/or corruption.

Robust systems, controls, procedures and processes will be established to ensure that the risk of impropriety is minimized through deterring and detecting fraud.

Staff and other stakeholders are encouraged to report any allegations or suspected fraud or corruption without fear of reprisals.

Allegations will be treated seriously and systematically, and will be effectively and promptly investigated.

Confidentiality, in so far as possible, will be maintained for all allegations made in good faith, and where reports are made anonymously, such anonymity will be respected.

Appropriate action, within the full extent of the law, will be taken against those that have been found guilty of being party to any illegal activity.

POLICY OBJECTIVES

Johannesburg City Parks and Zoo recognizes the sensitivity and the damaging consequences of fraud and corruption on the Company and its stakeholders.

The Policy strives to;

- Ensure that systems, procedures and processes exist in line with good governance, legislative, operational needs and industry norms and best practice to support the requirements of this policy.
- Ensure that management is aware of its responsibilities for identifying exposures to fraudulent activities and for establishing controls and procedures for preventing and/or detecting such fraudulent activity when it occurs.
- Provide guidance to employees as to action that should be taken where fraudulent activity is suspected.
- Provide clear guidance as to responsibilities for conducting investigations into fraudulent activities.
- Promote a culture of honesty, openness, and sound ethical behaviour

GUIDING PRINCIPLES (for measuring success)

- Loss of resources due to fraud, corruption and theft are minimised.
- Stakeholder's satisfaction is optimised.
- Clean audit reports
- The risks of fraud and corruption are identified and mitigation measures implemented.
- Successful disciplinary cases or where appropriate criminal prosecution against officials that have been found guilty.
- Reduction in the incidents of fraud and corruption.
- Employees being aware of what constitutes fraud and what steps to take when fraud has occurred or suspected.

SCOPE AND APPLICATION

This Policy applies to all staff members of JCPZ including contractors, service providers, suppliers and other stakeholders

ROLES AND RESPONSIBILITIES

Managing Director

- As the Accounting Officer of the organization and the principal custodian of the organization's assets and resources, the Managing Director is responsible for ensuring this policy is applied and adhered to.
- The Managing Director will ensure that full and unrestricted access is given to the Internal Audit and any external body requested to investigate. This includes the authority to immediately search the work area or individual in question, including any files and computers, without prior knowledge or consent.
- Wherein the investigation reveals that a JCPZ staff member has committed fraud, in consultation with the Legal Adviser and the Executive Manager: Corporate Services, the Managing Director will pursue disciplinary action in terms of JCPZ's disciplinary procedures. **(*Please refer to JCPZ disciplinary policy*),** or legal action. Where appropriate, criminal prosecution should be pursued.
- In the case of substantiated fraud, the Managing Director will take immediate steps to mitigate potential loss of JCPZ's reputation and credibility with donors/sponsors and partners who are involved in funding or delivering work in the particular context in question.

- For cases referred to the South African Police Services for criminal proceedings that are subsequently brought to court and the prosecution is successful, the Managing Director via the Executive Manager: Business Development, will produce a press release that should encourage the local newspapers to cover the story. For cases where the Managing Director is involved, the Board of Directors, via the Executive Manager: Business Development will produce a press release that should encourage the local newspapers to cover the story.
- In high profile cases of fraud, Stakeholder and Public Relations unit will manage and monitor any media response, and will release information only when it is approved by the Managing Director, in consultation with the Legal Adviser. In cases wherein the Managing Director is involved, the approval will be obtained from the Board.

Management

- Must establish and implement the internal controls to detect and deter fraud that are cost effective and commensurate with the magnitude of identified risks.
- Must promote an ethical and transparent environment that encourages staff members at all levels to actively participate in protecting the company's reputation and resources.
- Must eensure that all employees are made aware of JCPZ policy on fraud, corruption, theft and associated internal irregularities and for reporting suspected irregularities.
- Must strive to create an environment in which their staff feels able to approach them with any concerns they may have about suspected irregularities.
- Where JCPZ has suffered pecuniary loss or loss of other material assets, management must put measures in place to seek restitution from the individual(s) responsible for the fraud.
- Must expeditiously respond to reports issued by Internal Audit. In the case of recommendations being made after an instance of fraud and corruption, this is in order to reduce the risk of recurrence.

Employees

- Must report all incidents of actual or potential fraud, corruption, theft or irregular conduct as soon as they become aware of it to Management or the Managing Director.

  Should the staff member feel that reporting to Management or the Managing Director is inappropriate, then they can report directly to the GM: Internal Audit or the

Chairperson of the Audit Committee or the Chairperson of the Board, or through the "Anonymous Tip-Off" hotline.

- Must act in the best interest of the employer.
- Are bound by the company's Policies, Conditions of Service, Code of Conduct and Ethics as well as other codes issued by relevant professional bodies.

Internal Audit

The internal audit department has the primary responsibility to:-

- Investigate all reported and suspected fraudulent or irregular acts brought forward to their attention by the Fraud Committee as defined in the policy. If the investigation substantiates that fraudulent activities have occurred, the internal audit department will issue reports to the Head of Department of the alleged perpetrator and, if appropriate, to the Board of Directors through the Audit Committee.
- Decide on whether to refer the investigation results to the appropriate law enforcement and/or regulatory agencies for independent investigation in conjunction with legal advice and Executives, as will final decisions on disposition of the case.
- Raise fraud awareness raising and train employees on fraud prevention and detection. JCPZ will ensure that all employees are aware of their responsibilities for fraud control and ethical behaviour. Targeted training will be provided for new staff and refresher training for current staff.
- Proactively manage the overall risk of fraud

Audit Committee

Oversee JCPZ's internal controls and risk management practices.

Contractors/Suppliers/Consultants/Members of the public

JCPZ encourages the above interest groups who suspect fraud or corruption to report personally or in writing to the Managing Director, or to the Internal Audit Department or anonymously through the "Tip Off Anonymous" hotline.

Reports of fraud should include all known details, including all individuals alleged to be involved, the location, the time, and any relevant actions or statements.

11.2 WHISTLE BLOWING

POLICY STATEMENT

Johannesburg City Parks and Zoo encourages staff members and other stakeholders to disclose and report any allegations or suspected fraud or corruption without fear of reprisals (victimisation); will provide protection to all staff members and other stakeholders from reprisals or victimization for disclosures made without malice and in good faith, in defined circumstances and; will take appropriate action against those who report allegation maliciously.

THE POLICY APPLIES TO ALL EMPLOYEES, CONTRACTORS, SERVICE PROVIDERS, SUPPLIERS AND OTHER STAKEHOLDERS

POLICY OBJECTIVES

This policy aims to:

- encourage employees, contractors/service providers and other stakeholders to feel confident in raising serious concerns and to question and act upon concerns about practice;
- provide avenues for employees, contractors, service providers, suppliers and other stakeholders to raise those concerns and receive appropriate feedback on any action taken;
- ensure that employees, contractors/service providers and other stakeholders receive response to concerns and that they are aware of how to pursue them if not satisfied;
- reassure employees, contractors, service providers, suppliers and other stakeholders that they will be protected from possible reprisals or victimization if they have a reasonable belief that they have made any disclosure in good faith;
- ensure that systems and procedures are in place to support the requirements of this policy;
- promote a culture of honesty ,openness and sound ethical behaviour.

GUIDING PRINCIPLES (for measuring success)

- Loss of resources due to fraud, corruption and theft are minimised.
- Protection of employees who report allegations of fraud and corruption in good faith and without malice.
- Clean audit reports
- The risks of fraud and corruption are identified and mitigation measures implemented.
- Successful disciplinary cases or where appropriate criminal prosecution against officials that have been found guilty.
- Reduction in the incidents of fraud and corruption.
- Employees being aware of what constitutes fraud and what steps to take when fraud has occurred or suspected.

APPLICATION

This policy is designed to deal with concerns raised relating to fraud, corruption, misconduct and malpractice within JCPZ. The policy will not apply to matters of personal grievances, which shall be dealt with under the existing procedures set out in the Human Resources Policy and procedure manual of the Company. Details of these procedures are obtainable from the **Human Resources Unit.**

ROLES AND RESPONSIBLITIES

The Managing Director

- As the Accounting Officer of the organization and the principal custodian of the organization's assets and resources, be responsible for ensuring this policy is applied and adhered to.
- Must take appropriate action to protect the whistle blower from any harassment or victimization (including informal pressures) when raising concerns in good faith.
- Must ensure that the matter has been properly addressed and thus, subject to any legal constraints, will ensure that whistle blowers are informed of the outcome of any investigation.
- Must take appropriate disciplinary or legal action against an individual who makes an allegation frivolously, maliciously or for personal gain. Allegations made in good faith but not confirmed by the investigation will not result in disciplinary action being taken against individuals.

Management

- Must ensure that all employees are made aware of JCPZ's policy on whistle blowing.
- Must strive to create an environment in which the staff feels able to approach management with any concerns they may have about suspected irregularities.
- Must lead by example by following all relevant policies, procedures and code of ethics.

Whistle blowing is an essential element in the fight against fraud.

Employees

- JCPZ members of staff shall maintain the highest level of integrity and efficiency in all JCPZ activities and operations.
- Are expected to lead by example by following all relevant policies, procedures and the code of ethics.
- Can report any fraudulent activities either to management or the Managing Director. Wherein the employees feel that reporting to Management or the Managing Director is inappropriate they can report directly to the GM: Internal Audit on (011) 646 2000 Ext 209 or the chairperson of the Audit Committee or the chairperson of the Board or the anonymous tip-off line **0800 002 587 or** email: anticorruption@tip-offs.com or free fax at 0800 00 77 88/ **website www.ti-offs.com.**

Internal Audit

- Must treat all concerns with confidentiality and in confidence and make every effort, subject to any legal constraints, not to reveal the identity of the whistle blower. At the appropriate time, however, the whistle-blower may need to come forward as a witness
- Must respond to concerns brought forward by the Fraud Committee and all other channels.
- Immediately, upon receipt of an allegation, conduct a preliminary investigation to assess whether an in-depth investigation is appropriate
- Where appropriate, refer the matters to management or 3rd party found to be duly competent to conduct investigations.
- Must ensure appropriate communication of the outcome of the investigations and report to anyone with a legitimate need to know.

- Must provide regular training on this policy to new staff members and refresher training to current staff to make them aware of this policy and to encourage them to report possible irregularities as defined above.

Members of Public/contractors

JCPZ expects that its contractors and all stakeholders to maintain equivalent integrity and efficiency standards and will not tolerate prohibited practices in its activities or operations

What is whistle blowing?

Whistle blowing is the process by which employees or other individuals can raise a concern about serious malpractice within the company.

How do you blow the whistle?

The reporting channels for unethical conduct, fraud and corruption are the following:

- When an employee witnesses unethical conduct, fraud and corruption it must be reported to his immediate manager;
- Should the employee not be comfortable with this for any reason, e.g. that the manager may be involved, he should report it to superior of the manager concerned;
- If the employee wishes to remain anonymous, the report must be made to the Tip-Off Anonymous Line.
- External parties wishing to report matters are also encouraged to utilise the TOA.