



FRAUD PREVENTION POLICY

Document Ref.	12
Version No.	3a
Custodian	Board Secretary
Approved By	Operations Committee (OPSCOM)
Effective Date	17 November 2020

1. PURPOSE

The aim of this policy is to clearly communicate the IRBA's commitment to preventing and eradicating fraud throughout the organisation. In addition, it is to outline the organisational framework to prevent fraud; promote and reinforce existing legislation, systems, policies, procedures, rules and regulations of the IRBA; and describe the investigation and recovery of loss processes.

2. SCOPE

- 2.1 This policy is designed to deal with concerns raised by employees, members of the public, registered auditors, providers of goods and/or services and stakeholders in relation to fraud, corruption, misconduct and malpractice within the IRBA.
- 2.2 It must be read in conjunction with the relevant policies addressing grievances, disciplinary measures and unfair labour practices.
- 2.3 The management of fraud and corruption threats is the responsibility of everyone in the organisation.

3. LEGISLATIVE REQUIREMENTS

The IRBA's objective is to endeavour to protect the financial interests of the South African public and international investors in South Africa through the effective and appropriate regulation of audits conducted by registered auditors, in accordance with internationally recognised standards and processes. As a result, the IRBA endeavours to adhere to the highest standards of transparency and accountability.

Therefore, the IRBA recognises that in order to be successful in its mission, it has to strictly adhere to its enabling statute, the Public Finance Management Act and Treasury Regulations as well as the governance codes. In addition, the IRBA accepts that fraud is an operational risk and, as a result, commits itself to proactively combat fraud, including all other acts of dishonesty, on a zero-tolerance basis.

Section 51(1)(a) of the Public Finance Management Act stipulates that the Accounting Authority is responsible for ensuring that the public entity has and maintains effective, efficient and transparent systems of financial and risk management and internal control. Further, Section 27.2.1 of the Treasury Regulations requires that a risk assessment be conducted on a regular basis. In addition, a risk management strategy, which has to include a fraud prevention plan, must be compiled and used to direct internal audit efforts.

In light of the above, this policy has been designed in accordance with a number of South African laws

and guides that include, but are not limited to, the:

- 3.1 Public Finance Management Act 1 of 1999 and accompanying Treasury Regulations;
- 3.2 Protected Disclosures Act 26 of 2000;
- 3.3 Prevention and Combating of Corrupt Activities Act 12 of 2004; and
- 3.4 King Report on Corporate Governance.

4. DEFINITIONS

- Fraud** This is defined according to Section 34 of the Prevention and Combating of Corrupt Activities Act as the unlawful and intentional making of a misrepresentation which causes actual prejudice or is potentially prejudicial to another.
- Theft** In Section 34 of the Prevention and Combating of Corrupt Activities Act, this is defined as the unlawful appropriation of moveable corporeal property belonging to another, with intent to deprive the owner permanently of the property.
- Corruption** Chapter 2 of the Prevention and Combating of Corrupt Activities Act defines a general offence of corruption as an act that involves any person who gives or agrees or offers to give or accept any gratification amounting to an unauthorised or improper inducement to act or not to act in a particular manner.
- Misconduct** This defines financial misconduct in the handling or reporting of money, financial transactions or other assets.

5. POLICY PRINCIPLES

5.1. Fundamentals

- 5.1.1 The IRBA has adopted a zero-tolerance approach to fraud and corruption.
- 5.1.2 The IRBA will maintain appropriate controls for the prevention and detection of fraud and corruption.
- 5.1.3 Every person who falls within the scope of this policy has a duty to report any known or suspected conduct that constitutes or might constitute fraud and/or corruption.
- 5.1.4 All allegations of fraud and/or corruption shall be investigated without delay.
- 5.1.5 The Protected Disclosures Act protects an employee against dismissal or occupational prejudice, where a disclosure has been made to his/her employer in good faith and in accordance with a procedure prescribed by the employer that meets the requirements of

this Act (also refer to the Whistleblowing Policy). A copy of this legislation is available from the Board Secretary.

5.2 Roles and Responsibilities

- 5.2.1 Section 49(1-2) of the Public Finance Management Act, as amended, stipulates the following: *“Every public entity must have an authority which must be accountable for the purposes of this Act. If the public entity has a board or other controlling body, that board or controlling body is the accounting authority for that entity....”*
- 5.2.2 The Board is responsible for, among others, ensuring that a risk management strategy is in place and is clearly communicated to all employees.
- 5.2.3 The Board has delegated the Chief Executive Officer (CEO) as being responsible for the risk management strategy. The CEO is to be supported by the Directors, who are accountable to the Board in terms of its oversight responsibility and are responsible for implementing fraud and related policies as well as escalating identified fraud risks to the Board.
- 5.2.4 Employees are responsible for preventing and detecting fraud in the execution of their responsibilities.
- 5.2.5 The service provider responsible for the IRBA fraud hotline must inform the IRBA of any reports received.

FRAUD PREVENTION POLICY PROCEDURES

1. Reporting Procedures and the Resolution of Reported Incidents

1.1. *Fraudulent or Corrupt Acts and What Should be Reported*

1.1.1. Fraudulent or corrupt acts may include:

1.1.1.1 Systems issues: That is where a process/system exists and is prone to abuse by employees, the public or other stakeholders. Examples include:

- Statutory/regulatory non-compliance;
- Procurement fraud, e.g. irregular collusion in the awarding of tenders or orders for goods and/or services;
- Private interest in contracts;
- Deliberate non-compliance with the delegation of authority limits;
- Collusion in contracts management;
- Collusion in inspections; and
- Travel and subsistence fraud.

1.1.1.2 Financial issues: That is where individuals or companies have fraudulently obtained money from the IRBA, and examples are:

- Syndicate fraud, e.g. phishing scams, fake antivirus scams, etc.;
- Creditors fraud, e.g. diverting payments to incorrect creditors;
- Suppliers submitting invalid invoices or invoicing for work not done;
- Payroll fraud, e.g. the creation of “ghost employees”;
- Making a profit from insider knowledge; and
- Financial misconduct in the handling or reporting of money and financial transactions or other assets.

1.1.1.3 Equipment and resource issues: That is where IRBA equipment is utilised for personal benefit or is stolen, and examples are:

- Theft of assets, e.g. computers, etc.;
- Personal use of resources, e.g. telephones, the internet and e-mail;

- Irregular destruction, removal or abuse of records (including intellectual property); and
 - Leaking of confidential information, which causes actual prejudice or is potentially prejudicial to another.
- 1.1.2 Proven fraud and/or corruption transgressions shall be subjected to appropriate corrective action and/or sanction, including (where appropriate) consideration of:
- 1.1.2.1 In case of employees, taking disciplinary action within a reasonable period of time after the incident;
 - 1.1.2.2 Instituting civil action to recover losses;
 - 1.1.2.3 Initiating criminal prosecution by reporting the matter to the South African Police Service (SAPS) or any other relevant law enforcement agency;
 - 1.1.2.4 Action provided for in legislation governing the IRBA and its stakeholders; and
 - 1.1.2.5 Any other appropriate and legal remedy available.
- 1.1.3 Directors are required to ensure that if losses or damages are suffered by the IRBA, as a result of the reported acts committed or omitted by an employee or any other person, those losses/damages are recovered from such an employee or other person, if he/she is found to be liable.

1.2 What Should an Employee Do If They Suspect Fraud?

- 1.2.1 All employees are responsible for reporting all occurrences of corruption, fraud, theft, maladministration or illegal acts. Information received on the following categories of employees must be reported to the nominated/authorised persons:
- Directors, all employees and the Board Secretary to the CEO.
 - All employees (except the CEO, Directors and the Board Secretary) to the Board Secretary.
 - The CEO to the Chairman of the Board.
- 1.2.2 In addition to 1.2.1. above, employees who hold positions of authority and who know or should have reasonably known that another person has committed an act of corruption must report such knowledge or suspicion to any police official.
- 1.2.3 The employee or any other complainant may remain anonymous, in accordance with the provisions of the Whistleblowing Policy. Should employees wish to report allegations

of fraud anonymously, they should make use of the fraud hotline.

- 1.2.4 Care should be taken to avoid unsubstantiated, malicious, frivolous or mistaken allegations.
- 1.2.5 In addition, care should be taken to avoid alerting suspected individuals that an investigation is underway.

1.3 *What Should a Member of the Public, a Registered Auditor, Providers of Goods and/or Services or Stakeholders Do If They Suspect Fraud?*

- 1.3.1 The IRBA encourages members of the public, registered auditors, providers of goods and/or services or other stakeholders who suspect fraud to report such acts through the service provider, Whistle Blowers (which hosts the disclosure services), that has been appointed by the IRBA, the CEO, the Board Secretary or the Chairman of the Board.

1.4 *How Will Allegations of Fraud Be Dealt with by the IRBA?*

- 1.4.1 The action taken by the IRBA will depend on the nature of the concern. The matters raised may:
 - 1.4.1.1 Be investigated internally; or
 - 1.4.1.2 Referred to the SAPS or other relevant law enforcement agency.
- 1.4.2 Any alleged fraud committed by an employee or any other person will be pursued through an investigation and to the full extent of the law, including (where appropriate) consideration of:
 - 1.4.2.1 In case of employees, taking disciplinary action within a reasonable period of time after the incident;
 - 1.4.2.2 Instituting civil action to recover losses;
 - 1.4.2.3 Initiating criminal prosecution by reporting the matter to the SAPS or any other relevant law enforcement agency;
 - 1.4.2.4 Action provided for in legislation governing the IRBA and its stakeholders; and
 - 1.4.2.5 Any other appropriate and legal remedy available.
- 1.4.3 The Operations Department is required to ensure that losses/damages suffered by the IRBA, as a result of the reported acts committed by an employee or any other person, are recovered from such an employee or other person, if he/she is found to be liable.

1.5 Who Will Conduct the Investigation?

- 1.5.1 The authorised person will approach the Legal Department, which has the primary responsibility for the investigation of all suspected fraudulent acts, as defined in this policy.
- 1.5.2 If the investigation substantiates that fraudulent activities have occurred, the Legal Department will issue reports to the authorised person and, if appropriate, to the Board.
- 1.5.3 Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for an independent investigation will be made in conjunction with the Legal Department and the authorised person (only the CEO and/or Chairman of the Board), who will make the final decision on the disposition of the case.

2. Confidentiality

- 2.1 All received and investigated information relating to fraud will be treated with confidentiality. 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 in order to avoid harming the reputations of suspected persons who are subsequently found innocent of wrongful conduct.
- 2.2 Any employee who suspects dishonesty and/or fraud should not attempt to conduct investigations or interrogations themselves.
- 2.3 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 CEO.

3. Publication of Sanctions

- 3.1. The CEO, in consultation with the Chairman of the Board, will determine 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 other means.
- 3.2. The Chairman of the Board will report to the Board on all the disclosures made and the subsequent action taken.

4. Application of Prevention Controls and Detection Mechanisms

- 4.1. In respect of all reported occurrences of fraud, 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.

5. Creating Awareness

- 5.1. It is the responsibility of all Directors to ensure that all employees are made aware of and receive appropriate training and education with regard to this policy.

6. Implementation

- 6.1. The custodian of this policy is the CEO, who is supported in its implementation by all Directors of the IRBA.
- 6.2. The Board Secretary is responsible for the administration and revision of this policy.
- 6.3. The policy will be reviewed every year, in line with the risk management strategy.