THE SPAR GROUP LIMITED
Reg. No. 1967/001572/06
("the Company" or "SPAR")

FRAUD PREVENTION POLICY

INTRODUCTION

SPAR requires employees:

- to act honestly and with integrity at all times;
- to conduct all aspects of business at the highest level of professionalism, in line with the Company's value system (Entrepreneurship, Family Values and Passion);
- to safeguard the Company's resources, tangible and intangible assets; and
- to report unethical behaviour, fraud, theft, corruption, bribery or any associated irregularity ("crimes of dishonesty") relating to the Company.

SPAR does not tolerate any crimes of dishonesty and subscribes to the principles contained in the King report on Corporate Governance, best practice and relevant legislation aimed at combatting crimes of dishonesty, such as the Prevention and Combating of Corrupt Activities Act, 12 of 2014 ("PCCAA"). The Company complies with The Protected Disclosures Act, 26 of 2000, as amended, and all employees should be familiar with the contents of the Act.

PURPOSE

This policy is designed to:

- provide guidance to employees on what is regarded as crimes of dishonesty and how they should react should they be faced with unethical behaviour or conflicting situations during their business;
- ensure a consistent and effective approach to the process of fraud management; and
- minimise fraud occurrences within the Company.

It is important that SPAR be prepared to respond effectively to crimes of dishonesty and to limit loss or reputational harm.

SCOPE

This policy applies to all employees.

The board of directors of the Company is ultimately responsible for ensuring compliance with this policy and will be aided in this task by the Group Financial Director (GFD), Group Company Secretary (Cosec), Group Internal Audit Manager (IAM), Management, and the Company's respective Audit and Risk Committees' (A&RCo's).

Management and A&RCo's:

- recognize that it is their role to ensure proper management of crimes of dishonesty, as detection, prevention and appropriate reaction to incidents are of vital importance for the Company;
- are committed to ensuring that all incidents are investigated and affirm that the persons who are tasked with the responsibility of investigating these incidents will be supported in their function; and
- need to ensure that there is effective response to all reports of crimes of dishonesty and those employees and third parties who are guilty of crimes of dishonesty are dealt with appropriately.

Management:

- should be familiar with the types of improprieties that may occur within their area of responsibility and be alert thereto;
- are responsible to enforce and monitor compliance with this policy;
- are obliged to refer to this policy and act in terms thereof when incidents of potential crimes of dishonesty are reported; and
- are accountable and responsible to ensure that all reasonable steps are taken to prevent and detect instances of crimes of dishonesty in their specific areas.

A zero-tolerance approach and an effective response to all incidents of crimes of dishonesty should lead to a reduction in crimes of dishonesty within the Company.

This policy is to be read in conjunction with SPAR's Code of Ethics, Anti-Bribery and Corruption Policy, Whistleblowing Policy and Disciplinary Code and Procedure, including other processes and procedures manuals for Finance, Human Resources, Logistics and insurance.

DEFINITIONS

Corruption refers to the misuse of entrusted power for private gain. Corruption occurs when any person who, directly or indirectly:

- accepts or agrees or offers to accept any gratification from any other person, whether for the benefit of himself or herself or for the benefit of another person; or
- gives or agrees or offers to give to any other person any gratification, whether for the benefit of that other person or for the benefit of another person.

Examples of corruption include, but are not limited to:

- collusion with a supplier to inflate prices;
- threatening suppliers to termination of a business arrangement should the supplier be reluctant to pay kickbacks;
- failure to disclose one's involvement/interest upfront with a supplier or customer; and
- any situation where an employee, relative or friend of an employee, or any other person acting as a nominee for an employee or any aforementioned persons, receives goods, services, reward in return for the employee's assistance in procuring for a third party a benefit from the group's assets, operating performance, etc.

Employee refers to any staff member, member, agent, consultant or person acting on behalf of the Company, who receives payment, either full or part time, from the Company. The term includes any volunteer who provides services to SPAR through an official arrangement with the Company.

Fraud refers to the unlawful and intentional making of a misrepresentation, which causes actual and/or potential prejudice to another. For the purposes of this policy, fraud shall include, but is not be limited to:

- forgery or the deliberate alteration of documents for fraudulent purposes (application forms, contracts, cheques, purchase orders, etc.);
- misrepresentation of information on documents;
- any deliberate irregularity in the handling or reporting of monetary transactions;
- authorising or receiving payments for goods not received or services not rendered;
- an intentional or deliberate act to deprive the Company of value, or to gain an unfair benefit using deception, false suggestions, suppression of truth, or other unfair means which are believed and relied upon;
- unlawful and/or irregular activities (blackmail or extortion, accepting or offering bribes, submitting false claims for payment or re-imbursement);
- electronic crimes or irregularities;
- the unauthorised use of the Company's assets for personal gain;
- contravention of any money laundering legislation;
- unlawful and or irregular disclosure of information pertaining to SPAR;
- insurance fraud; and
- wilful negligence intended to cause damage to the material interests of the Company.

Management refers to the designated members of executive management or his/her delegee, designated departmental heads or their delegees and designated specialists.

Theft refers to the unlawful misappropriation of moveable property or money with the intention to steal. Examples of theft include, but are not limited to:

- theft, disappearance or destruction of any asset without authority;
- misappropriation of funds, securities, supplies or any other assets; and
- unauthorised removal of money, inventory, assets, stationery and other consumables.

FRAUD MANAGEMENT

There are five phases of fraud management, namely, fraud risk assessment, prevention, detection, investigation and recovery and mitigation.

Fraud Risk Assessment

To identify potential fraud threats and implement appropriate measures

All business units in the performance of their own risk assessments should include an assessment of potential fraud risks and how to mitigate those risks.

Prevention

Actions taken to deter or prevent fraud from occurring

It is noted that fraud and related crime prevention techniques fall into three disciplines:

- **Operational control**, that addresses related risk exposures and embraces related financial and audit controls, personnel selection and monitoring techniques.
- **Physical security**, that deals largely with visitor control (restricting access to sensitive areas by unauthorized employees, members of the public, firearms, drugs, etc.).
- **System security**, that concentrates on improper usage of computer systems, e-mail facilities, password control, authorisation, logging off, encryption and message authentication.

It is the responsibility of all management to ensure that adequate preventative controls are designed, documented and implemented to prevent fraudulent activity. The following procedures are typical preventative measures:

- sound recruitment and selection procedures to ensure that the right calibre of employee is appointed. All employees should be screened before they are appointed. Previous employment checks should be conducted, noting names and positions of people from whom information was gained. The report of such information gathered must be kept in the employee records at Human Resources;
- detailed job descriptions in place to ensure that employees understand fully what their responsibilities entail and the extent to which their authority entails;
- regular taking of leave by employees;
- regular supervisory review of employees in positions of trust;
- detailed system descriptions in place to ensure that all employee members are aware of their impact and roles within the control system;
- weaknesses in systems or poor work performance identified, and necessary corrective action taken;
- segregation of incompatible duties is extremely important;
- employees to have clear delegation of accountability, authority and responsibility;
- special attention given to critical risk exposures and effectiveness of controls in high risk areas;
- management constantly aware of any areas of exposure or which are prone to high risk;
- cautious about accepting things on face value. Question statements made, logic, etc;
- areas indicating high management tumover, and where subsequent loss of management or intemal control could occur should be identified, addressed and carefully monitored;
- management's close involvement in the day-to-day activities of the business of the group;
- the basic attitude of employees and occurrences of minor irregular incidents could be indicators of more serious underlying problems;
- becoming aware of basic fraud indicators (red flags);
- maintaining a record of irregular incidents and identifying high risk area; and
- adopting a zero-tolerance approach to all employees who commit crimes of dishonesty.

Management should promote an anti-fraud working environment through:

- creating an environment which is intolerant to fraud;
- communication to and training of employees to ensure awareness of this policy and the Whistleblowing Policy.

Detection

Actions aimed at uncovering or revealing the presence of fraud or fraud attempts

It is the responsibility of all management to ensure that adequate controls to detect fraudulent activities are designed, documented, communicated and implemented. This can also be achieved

by creating and maintaining an awareness of the Whistleblowing Policy, including the Whistleblowing Hotline.

Investigation

Gather evidence and build a case to stop the perpetrator, recover assets, obtain resolution, and facilitate successful prosecution and conviction

SPAR's policy is to promptly investigate all crimes of dishonesty perpetrated within or against the Company and to pursue legal remedies for the recovery of any losses and for the conviction of guilty parties. Crimes of dishonesty may not be treated as acceptable policy and must be identified and dealt with appropriately.

Management should exercise their discretion to determine the nature and extent of resources applied to the investigation process. Before commencing investigation, management must seek guidance from the IAM on the proposed investigation.

All investigations must be treated as strictly confidential.

Recovery and Mitigation

Action taken to recover assets or losses, stop fraud and avert further losses resulting from the fraud

Employees who commit fraud are in material breach of the contract of employment amounting to gross misconduct and will be subjected to appropriate disciplinary action, in accordance with Human Resource polices.

SPAR will pursue all appropriate action to the full extent of the law.

When a fraud occurs, SPAR Group Audit Services (SGAS), together with management will immediately review all relevant controls in order to prevent similar frauds occurring and communicate it to all business units.

REPORTING

All employees have a general duty to act in the best interest of the Company. It is therefore essential that reports of crimes of dishonesty be routed through a central "reporting channel" to ensure effective and consistent response. It is anticipated that the following will be the sources of reports:

- Employees may approach their line manager or supervisor or Distribution Centre Managing Director (DC MD) or the Chief Executive Officer (CEO) of SPAR directly.
- Employees may also approach the Cosec, IAM or SGAS directly.
- All direct reports received by line managers and supervisors must immediately be conveyed either verbally or in writing to the IAM. Verbal reports must be confirmed in writing.
- Suppliers or customers may approach the DC MD, CEO, IAM, Cosec or SGAS directly.
- All offenses greater than R100 000 are required to be reported to the South African Police Services, in terms of the PCCAA.
- In instances where employees, suppliers or customers wish to remain anonymous, they should report crimes of dishonesty through the **Whistleblowing Hotline**:

Free call: 0800 864 616
Email: spar@tip-offs.com
Web: www.tip-offs.com

The hotline is set up in such a way that all Distribution Centre related crimes of dishonesty reports are immediately communicated to the relevant Distribution Centre Human Resources Manager, IAM and Cosec, and for Central Office reports to the IAM and Cosec.

Under no circumstances may any person who receives a report fail to convey the report or act on the reported suspicion without referring it to either of the above.

No information with regard to the issues covered within this policy may be shared with any third parties or the media. The GFD, where applicable, will be responsible for any necessary disclosures to any third parties as required by the law.

Annexure A provides steps that should be utilised as a guideline when an incident is reported.

ADMINISTRATION OF THIS POLICY

The custodian of this policy is the Group Secretariat Department who will be responsible for the administration, revision, interpretation and application of this policy, which will be reviewed triennially or as and when required.

Any alternation of this policy is subject to approval by the Board/Audit Committee.

This policy was approved by the Board on **21 May 2021** and becomes effective immediately on approval.

Annexure A

Step 1

When an incident is reported to any of the sources mentioned above, the following course of action will be taken:

- All Information Communication Technology (ICT) related fraud will be investigated by external consultants.
- Allegations against the DC MD, GFD, Cosec, IAM or any Executive Committee member should be referred to the CEO, and will be investigated by external investigators, should an investigation be necessary.
- Allegations against the CEO or any board member (other than the Chairman), should be referred to the Chairman of the Board.
- Allegations against the Chairman of the Board should be referred to the Chairman of the Audit Committee.

The mandate of the SGAS only allows preliminary investigation of crimes of dishonesty relating to management level (D-Band) and lower levels.

Management, in liaison with forensic investigators (if appointed), must take appropriate action to prevent the continuance of the crimes of dishonesty. Such actions may include, but is not limited to, immediately removing records and placing them in safe custody, limiting access to the location where the records reside, and preventing the individual/s suspected of committing the crime from having access to the records.

Step 2

An assessment of the incident should be completed by the DC MD or CEO and he/she must consider the merits of the information provided by the complainant.

Based on the assessment completed, the DC MD or CEO, will determine how the incident will be dealt with and support whether a preliminary investigation should be conducted. The DC MD or CEO should:

- engage who should conduct the investigation;
- establish the scope and objectives of the investigation; and
- set timeframes.

SGAS may be called upon to assist with the completion of a preliminary investigation should the DC MD or CEO elect not to utilise internal resources.

The suspension or temporarily transfer of the suspect to ensure the security of evidence must be determined in consultation with Human Resources. It is important that consideration be given to the financial and reputational implications of suspension, but the principle of ensuring the security of evidence must remain paramount where there is doubt. It is accepted that the Human Resource department will ensure that steps are taken in terms of accepted and fair procedure.

Step 3

The DC MD or CEO must inform the GFD and IAM in writing of the incident reported and how the preliminary investigation will be conducted. A detailed explanation and rational must be provided, should it be elect not to peruse the matter or conduct any further investigations.

Step 4

A preliminary investigation should be conducted based on the scope provided by the DC MD or CEO. The purpose of the preliminary investigation would be to:

- determine the legitimacy of the allegations;
- identify the perpetrator;
- identify the modus operandi;
- identify control weaknesses;
- secure any evidence found;
- prevent any or any further reputational damage; and
- quantification of the value involved and/or loss incurred.

In relation to the securing of evidence, a person must be given the responsibility of ensuring that the following steps are taken:

- access to personal computers, the computer system and documentation must be revoked;
- the personal computer of the suspect should be secured. See the guidelines below with respect to the securing computer evidence; and
- any assets in possession of the suspect should be secured (including cell phone, if company provided).

It is imperative that minimal disruptions to operations take place during the preliminary investigation stage. Based on the on the preliminary investigation completed a report should be complied detailing what was completed during the investigation and what the findings were.

Step 5

An assessment should be completed by the DC MD or CEO based on the preliminary investigation report. It should be established whether the matter requires detailed investigation or any other investigative resources.

Should it be decided to investigate the matter further, the DC MD or CEO should provide a mandate regarding:

- scope and objectives of investigation;
- timeframes; and
- resources required.

The preliminary investigation report should be submitted to the GFD and the IAM, in addition to any further investigative work to be conducted.

Step 6

Should the DC MD or CEO decide to investigate the matter further, the investigation should be conducted based on the mandate provided. The use of the following tools, techniques and resources should be considered:

- information and intelligence gathering tools;
- conducting of background checks;
- tracing of assets;
- interviewing witnesses;
- use of legitimate covert operations;
- use of computer technology;
- use of experts – e.g. forensic investigators;
- use of specialist investigative techniques – e.g. polygraph testing; and
- Interviewing the perpetrator.

Based on the on the detailed investigation completed a report should be complied detailing what was completed during the investigation and what the findings were.

Step 7

An assessment should be completed by the DC MD or CEO based on the detailed investigation report. It should be established whether the incident reported was factual, whether recourse and the possible recovery of loss is mandatory. Should it be established that recourse and the recovery of loss is required, consideration should be given to the following aspects:

- internal disciplinary action;
- civil litigation;
- criminal prosecution;
- Insurance claims; and
- Alternative dispute resolution.

In addition, controls, control improvements and remediating actions should be instituted to prevent the reoccurrence of the same or similar incident and communicated to all group entities (as required) for implementation.

Step 8

A final consolidated report should be prepared, and the report approved by the DC MD or CEO. The final report should detail:

- the scope and objective of the investigation;
- the resources utilized to complete the investigation;
- the issues addressed;
- findings;
- conclusions;
- recourse against perpetrator;
- Loss recovery and
- recommendations in terms of prevention of reoccurrence.

The final investigation report is to be provided to the GFD and the IAM.

Notes:

Initial securing of evidence and detailed investigation

- As this is a critical phase it is important that the task be allocated to a person with the necessary ability and experience to ensure that all the relevant information is obtained.
- Regards should be taken with respect to the collection of computer evidence.
- The securing of computer evidence must be performed by external consultants.
- The report back must be based on facts and not hearsay.
- The engagement of Forensic Assistants should be authorised by the DC MD or GFD, unless the investigators were engaged by the CEO.

Decision to suspend a supplier

- The DC MD must make the final decision to suspend a supplier on a regional level in consultation with the Regional Marketing Executive. All suppler suspensions must be communicated to the Group Marketing Executive.
- The Group Marketing Executive must make the final decision to suspend a supplier on a national level in consultation with the DC MD, GFD and CEO.

Decision to prosecute and seek to recover assets

Consideration should be given to use legal practitioners for the recovery of assets as required to ensure that losses or damages suffered by SPAR because of all reported acts committed or omitted if he/she is found to be liable for such losses.

Decision to suspend or transfer suspected employees

In consultation with the Regional and/or Group Human Resources Executive it should be determined whether the suspect should be suspended or transferred.