OPGCR - SL

OPERAÇÕES GCR – PRESTAÇÃO DE SERVIÇOS E LOGÍSTICA

Procurement - Manpower - Assistência Técnica - Logística

OPERAÇÕES GCR-PRESTAÇÃO DE SERVIÇOS E LOGÍSTICA

Risk & Fraud Management Policy

Contents

1

INTRODUCTION

1.1. DECLARATION
1.2. FRAUDE

2

POLICY DETAILS

2.1. EXEMPLES
2.2. BOARD OF DIRECTORS STATEMENT ON FRAUD
2.3. RESPONSABILITIES
2.4. DECLARATION OF INTERESTS
2.5.FRAUD RISK ASSESSMENT
2.6. MONITORING OF INTERNAL CONTROL SYSTEM
2.7. RECRUITMENT OF EMPLOYEES
2.8. COMMUNICATION AND TRAINING
2.9. INVESTIGATIONS
2.10. POLICY REVIEW

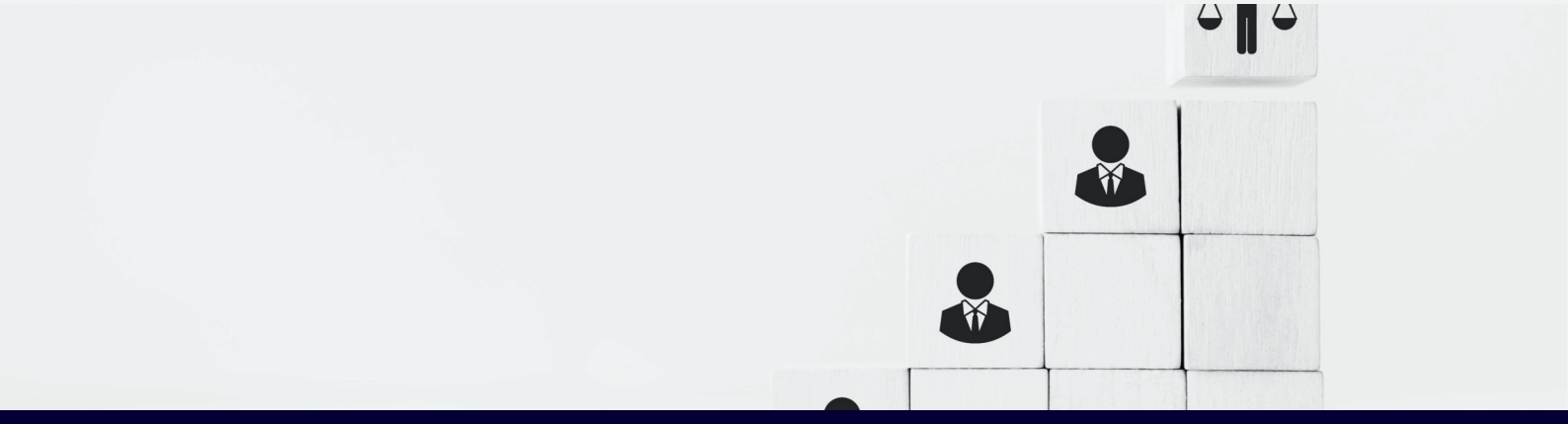
3

CONCLUSION

4

APPENDICES

4.1. APPENDIX A- EXAMPLES OF TYPES OF FRAUD
4.2. APPENDIX B- OFFERS / CONFLICT OF INTEREST
4.3. APPENDIX C- FORM: OFFERS, CONFLICT OF INTEREST AND AUTHORIZADTION
4.4. APPENDIX D - ADDITIONAL CONSIDERATIONS



1.Introduction

1.1 DECLARATION

OPERAÇÕES GCR, a company dedicated to providing services and logistics, is firmly committed to upholding the highest ethical and legal standards. The integrity of its personnel is fundamental to the company's success, ensuring professionalism, competence, and trustworthiness in all operations. The Fraud Risk Management Policy, effective from July 16, 2021, outlines the company's stance on fraud and the procedures to address such issues. This policy applies to all employees, service providers, and third parties acting on behalf of the company, collectively referred to as "employees."

In the event of fraud or non-compliance with the policy, disciplinary actions or termination may be imposed, and cases may be reported to the appropriate authorities. Any employee suspecting fraud or misconduct is required to report such incidents to the **OPERAÇÕES GCR** Chartered Accountant, who will escalate the complaint to the Board of Directors for further action.

The company is responsible for conducting thorough investigations to uncover the truth and implementing necessary measures based on investigation findings. The Board of Directors plays a crucial role in developing and enforcing anti-fraud policies, encompassing prevention, detection, and response mechanisms for addressing instances of fraud and irregular behavior.

1.2 FRAUD

For the purposes of this Policy, fraud is defined as any illegal or dishonest act committed with the intent of gaining an advantage or evading a responsibility. It involves deliberate deception or misrepresentation, leading to potential losses for the company. Fraud can manifest internally or externally and may involve employees, service providers, customers, suppliers, or other third parties acting alone or in collaboration with others.For the purposes of this Policy, fraud is defined as any illegal or dishonest act committed with the intent of gaining an advantage or evading a responsibility. It involves deliberate deception or misrepresentation, leading to potential losses for the company. Fraud can manifest internally or externally and may involve employees, service providers, customers, suppliers, or other third parties acting alone or in collaboration with others.

2.Policy Detail

3

This Policy is defined with the following elements:

- Exemples
- Statement by the Board of Directors regarding fraud
- Responsabilities
- Declaration of Interest
- Fraud Risk Assessment
- Monitoring of the Internal Control System
- Recruitment of employees
- Communication and training
- Investigations
- Policy Review
- Links

2.1. EXEMPLES

Fraud can involve various types of misconduct, such as embezzlement of funds or assets and manipulation of financial statements. Examples include accounts payable fraud, fake suppliers, personal purchases, accounts receivable fraud, procurement fraud, payroll fraud, vendor fraud, and wire transfer fraud. Some examples of types of fraud and corruption are provided in Appendix A.

2.2. BOARD OF DIRECTORS STATEMENT ON FRAUD

The Board of Directors of OPERAÇÕES GCR is dedicated to upholding the highest ethical and legal standards, implementing control procedures, and responding to dishonest behavior in accordance with relevant legislation and codes of conduct. Fraud is unequivocally intolerable within the organization.

2.3. RESPONSABILITIES

Anti-Fraud Policy

All employees are responsible for preventing and detecting potential fraud within the Company. Compliance with this Anti-Fraud Policy is mandatory for all employees.

Management assumes responsibility for ensuring this Policy is followed within their respective departments and business areas. The Board of Directors is responsible for designing and implementing anti-fraud policies, which include mechanisms for preventing, detecting, and responding to fraud and misconduct.

Reporting Suspected Fraud

All employees have an obligation to promptly report any suspected fraud, misconduct or irregular acts. Failure to report suspected fraud may be considered misconduct itself.

Complaints should be made to the Statutory Auditor of **OPERAÇÕES GCR** via sealed letter or email (manager@operacoes-gcr.com) with the subject "Fraud **OPERAÇÕES GCR**". The identity of the reporting employee will be kept confidential to the extent possible.

Anti-Fraud Coordinator

The Anti-Fraud Coordinator is responsible for investigating reports of suspected fraud and misconduct. The Coordinator will maintain the confidentiality of the reporting employee and ensure a thorough and impartial investigation is conducted.

Employees found to have committed fraud or misconduct will face disciplinary action up to and including termination of employment. The Company may also pursue legal action to recover any financial losses and report the misconduct to law enforcement where appropriate.

This Anti-Fraud Policy will be reviewed periodically to ensure it remains effective in preventing, detecting and responding to fraud and misconduct within the Company.

2.4. DECLARATION OF INTEREST

Management and employees have a duty to act in the best interests of **OPERAÇÕES GCR** and adhere to the current Code of Ethics. Potential conflicts of interest can arise when personal or family interests intersect with the company's interests. Therefore, all employees, including the Administration, must disclose any interests or family ties with entities related to the Company, such as other group companies, customers, suppliers, and external entities. Both Management and employees should reject any offers that could be seen as attempts to influence the company or the individual. A declaration of interest form (Appendix C) will be provided to all employees, including the Administration, to be completed and submitted to the anti-fraud coordinator when this policy is introduced or updated.

In cases of conflict of interest, employees should promptly disclose any potential conflicts to the colleague involved or withdraw from the relevant process and subsequent activities. Following an assessment by the Administration, the employee may be allowed to resume involvement in the process if deemed appropriate. Failure to disclose an existing interest or personal connection would constitute a violation of the Policy, leading to disciplinary or legal actions as applicable. It is advisable for employees unsure about what to declare or needing to update their declaration to err on the side of caution and seek guidance from their Department Administrator. The declaration should be kept in the employee's file, accessible only by the employee, Human Resources, and Administrators, unless legal obligations dictate otherwise.

2.5. FRAUD RISK ASSESSMENT

Fraud risk can exist in areas without a history of fraud losses, making historical cases an incomplete indicator of all potential fraud risks. Therefore, it is crucial for the Company to identify, assess, and implement strategies to mitigate fraud risks effectively.

To maintain an updated fraud risk assessment, the Board of Directors or an accredited entity subcontracted for this purpose should be responsible for conducting an annual review, or more frequently in the event of significant changes in the operating environment, risk profiles, and control matrices. This review involves examining procedures across all areas/departments of the Company and testing the effectiveness of identified controls to ensure they function as intended and consistently over time.

The developed work plans should encompass the following key points:

- Understanding the business and operational support processes by engaging in meetings/interviews with key personnel to review processes and associated documentation.
- Identifying and evaluating fraud risks for each Company process using appropriate risk assessment criteria to determine the likelihood and impact of potential occurrences.
- Utilizing the Risk Assessment Matrix to document the outcomes of fraud risk assessments.
- Formulating recommendations to mitigate fraud risks effectively.

Ultimately, the Board of Directors or the accredited entity responsible for the assessment should present the results of the fraud risk assessment, highlighting key findings and proposed risk mitigation strategies to enhance the Company's fraud prevention measures.

2.6. MONITORING OF THE INTERNAL CONTROL SYSTEM

The Board of Directors oversees OPERAÇÕES GCR's Internal Control System, ensuring it stays current with the Company's evolving environment by periodically reviewing and updating measures in place.

2.7. RECRUITMENT OF EMPLOYEES

When recruiting new employees with a focus on prevention, it is essential to request the following information:

- Criminal record
- References from former employers
- Original documentary evidence of the qualifications presented, such as a Certificate of Qualifications.

2.8.COMMUNICATION AND TRAINING

All employees must be alert to the possibility of fraud situations and participate in appropriate training and awareness actions on the matter to be better positioned to help prevent, detect, and respond to potential risks. **OPERAÇÕES GCR** is committed to ensuring that all employees are aware of their responsibilities. Thus, these training and awareness actions are an essential part of fraud prevention and should be designed to:

- Promote an anti-fraud culture from the Company's Administration to the employees.
- Communicate the responsibilities defined in this Policy to all employees.
- Provide employees with the necessary tools to identify fraud warning signs.
- Ensure that employees are aware of the fraud reporting mechanisms as documented in this Policy and the Code of Ethics.

Continuous Training

Fraud awareness actions are necessary to ensure that employees are aware of the issues relevant to preventing and detecting potential fraud. Training actions can be included in the daily training and must refer to all relevant information included in the Company's policies and procedures.

Continuous Communication

Continuous communication is necessary to keep employees aware of potential fraud risks to which the group is exposed and to remind them how to react if they identify any suspicious situation. All major policies and procedures regarding this matter are kept in a shared folder on the website (https://www.operacoes-gcr.com/commitments), were duly communicated and are available for consultation by all employees

2.9. INVESTIGATIONS

All suspected fraud must be thoroughly investigated, involving the analysis of reported incidents and the identification of responsible parties through a comprehensive investigation process.

2.10. POLICY REVIEW

This policy must undergo a review, at least once every two years, by the Administrator responsible for the Administrative area or by an external entity duly accredited for this purpose, under the supervision of the Administrator. Any revisions to this policy must also receive approval from the Board of Directors of **OPERAÇÕES GCR.**

2.11. LINKS

More information on these matters can be obtained from the following sources: Code of Ethics of OPERAÇÕES GCR (https://www.operacoes-gcr.com/commitments)

3.Conclusion

A successful strategy for preventing fraud, misconduct, and related infractions involves creating an environment that inhibits these types of violations. It is the responsibility of each employee to contribute to this environment.
While the specific circumstances of potential fraud may vary, it is crucial that all suspicions are investigated thoroughly and that appropriate actions are taken in response to confirmed incidents.
An employee who is vigilant and alert to the possibility of fraud or irregular situations is a powerful tool in mitigating these risks. Fraud prevention should go beyond basic regulatory requirements and utilize advanced controls to collect as many signals as possible, such as device verification, IP address validation, VPN monitoring, document and biometric verification, and more.
By mitigating potential risks before they arise, organizations can ensure that clients' accounts are fortified against fraudulent activities from the outset. The most effective method to prevent fraud is to inhibit malicious actors from gaining access to the system in the first place.
Fraud prevention efforts should be paired with fraud detection to identify the main fraud trends faced by the organization. As soon as new and trending fraud schemes are identified, teams need to work closely to turn fraud detection into fraud prevention.
Regular updates to fraud thresholds based on observed behavior, link analysis to identify patterns faster, and a complete process for managing fraud on the platform can help limit fraud losses. Establishing limits on repeat fraudsters, monitoring checks, investigating cases, and performing link analysis are key strategies.
By creating an environment that inhibits fraud, investigating all suspicions thoroughly, and empowering vigilant employees, organizations can effectively prevent fraud, misconduct, and related infractions.

4.Appendix

4.1. APPENDIX A – EXAMPLES OF TYPES OF FRAUD

Fraud is a pervasive issue that can manifest in various forms, causing significant financial losses and reputational damage to individuals, businesses, and financial institutions. This response will provide an overview of different types of fraud, including those related to company funds and assets, financial statements, and corruption.

Fraud Involving Company Funds and Assets

This type of fraud encompasses a range of activities, including:

- Theft of money
- Illegal transfer or embezzlement of funds
- Unauthorized use of checks and orders payable
- Forgery and duplication of invoices to generate false payments
- Misappropriation or misuse of assets
- False work appearance
- False expenses in service and/or on behalf of the company (e.g., hotels, meals, travel)
- Unauthorized payment of bonuses/prizes to employees
- Theft or unauthorized dissemination of sensitive/privileged information
- External fraud by someone in the public domain (e.g., false claim of a discount).

Fraud in Financial Statements

Fraud in financial statements results from intentional distortions or omissions of amounts or disclosures in financial reporting to mislead users. This can include:

- Falsification or alteration of accounting records or supporting documents
- Misrepresentation or intentional omission of relevant events, transactions, or other information
- Intentionally misapplication of accounting principles relating to amounts, classifications, modes of presentation, or disclosures

Corruption

Corruption involves the practice of any act or its omission, whether lawful or unlawful, against the receipt or promise of any compensation other than due, to the self or to a third party. Forms of corruption include:

- Collusion between internal employees and suppliers
- Receipt of goods and services through collusion
- Payment for work not carried out resulting from an agreement between the company and supplier
- Influence peddling
- Embezzlement (embezzlement and theft of public funds by those in charge)
- Abuse of power
- Economic participation in business
- The bribe
- Concussion (extortion committed by a public employee in the performance of their duties).

Other Types of Fraud

Other notable types of fraud include:

- Identity theft: stealing personal financial information to make fraudulent charges or withdrawals.
- Investment fraud: selling investments or securities with false, misleading, or fraudulent information.
- Mortgage and lending fraud: using false information or deceptive practices to obtain a mortgage or loan.
- Mass marketing fraud: using mass mailings, telephone calls, or spam emails to steal personal financial information or solicit contributions and fees.
- Bank fraud: the misuse of a financial institution or its services for personal gain, including counterfeiting, check fraud, identity theft, loan scams, credit card fraud, and phishing.
- Securities fraud: criminal activity that can include high-yield investment fraud, Ponzi schemes, pyramid schemes, advance-fee schemes, foreign currency fraud, broker embezzlement, pump-and-dumps, hedge-fund-related fraud, and late-day trading.

It is essential for individuals and businesses to be aware of these various types of fraud and to take steps to protect themselves from becoming victims. This includes implementing security measures, such as identity verification, fraud detection and prevention procedures, and anti-fraud monitoring systems. Additionally, reporting fraudulent activities to the appropriate agencies and law enforcement is crucial in preventing further financial losses and bringing perpetrators to justice

4.2. APPENDIX B – OFFERS / CONFLICT OF INTEREST

Offers and Conflict of Interest Policy

The company's policy on offers and conflict of interest aims to maintain the highest ethical standards and protect the integrity of the organization. Key points include:

- Employees must refuse any offers to themselves or third parties that could be seen as an attempt to improperly influence the company or employee.
- All employees must avoid conflicts of interest. A conflict arises when an employee's personal, financial or other interests could impair their ability to perform their duties objectively and in the best interests of the company.
- Examples of conflicts include an employee being involved in a decision process related to a company they have collaborated with, or a company owned by a family member.
- If a potential conflict of interest arises, the employee must obtain written authorization from management before proceeding.
- All conflicts of interest must be promptly reported using the company's declaration of interest form (Appendix C).

The policy emphasizes that employees must act with integrity, loyalty and due care in fulfilling their responsibilities to the company. Disclosing potential conflicts protects both the employee and the organization

4.3. APPENDIX C–FORM: OFFERS,CONFLICT OF INTEREST AND AUTHORIZATION

Offers and Conflict of Interest Policy

The company's policy on offers and conflict of interest aims to maintain the highest ethical standards and protect the integrity of the organization. Key points include:
Disclosing potential conflicts protects both the employee and the organization

Personnal Details

Name:
Department / Function:
Phone:
E-mail:
Date:

☐ I declare that I have read this Fraud Risk Management Policy and that I do not have any kind of conflict of interest.

☐ I declare that I have read this Fraud Risk Management Policy and that I have the following conflict(s) of interest.

Details of potencial conflict of interest or offers

Details	
Full name and details of company and people responsible for the offer or potencial conflict of interest	
LIst of people above with: • **OPERAÇÕES GCR** • **Benefit Recipient**	
Benefit amount	

Authorization

When evaluating an application, the authorizing person must assess how benefits or potential conflicts of interest may impact the applicant's or another person's conduct. Any benefit perceived as a bribe or contrary to the law must be rejected and formally presented to the hierarchical superior or Board of Directors for approval.

Decision Details	
Name of the person responsible for authorization	
Contact	
Required conditions (eg: date of receiving the benefit, value, etc.)	
Signature of the applicant	
Signature of the person responsible for the authorization	

his form must be delivered to the Board of Directors, and the employee must keep a copy of it.

4.4. APPENDIX D – ADDITIONAL CONSIDERATIONS

Additional information to the provisions of Section 2.4 of this Policy, with some examples of elements to be taken into account in an investigation situation.

Determine the main facts - veracity and credibility of the allegations	☐
Consider internal controls that may have been violated	☐
Consider any violation of the policies and procedures of the OPERAÇÕES GCR	☐
Consider initial evidence and its preservation	☐
Consider protecting documents and records (information collection process)	☐
Identify and secure digital evidence	☐
Preparation of the investigation plan	☐
Consider the most appropriate methods for gathering evidence	☐
Consider continuous manipulation	☐
Consider the company's management and the necessary documentation	☐
Consider applicable laws and regulations	☐
Consider the possibility of resorting to an external entity – Lawyers/Researchers	☐
Consider reporting to external entities – Police and additional reporting to the regulator	☐
Determine if the offense was committed and identify the situations that led to its practice	☐
Consider possible solutions and necessary actions	☐
Consider sanctions to be applied	☐
Consider company reputation and public interest issues	☐

THANK YOU MESSAGE FOR REVIEWING FRAUD RISK MANAGEMENT POLICY

Thank you for taking the time to review our fraud risk management policy. Your commitment to understanding and upholding our organization's protocols for detecting and preventing fraud is greatly appreciated. By familiarizing yourself with these guidelines, you play a crucial role in safeguarding our company's assets and reputation. Should you have any questions or require further clarification, please do not hesitate to reach out. Together, we can maintain a secure and trustworthy environment for all stakeholders. Thank you for your diligence and dedication to ensuring our continued success.

OPERAÇÕES GCR - S & L
NIF:5000673633
LUANDA-ANGOLA

Godzua Cornélio Rodrigues

Godzua Cornélio Rodrigues

Founder / CEO

OPGCR S&L

CONTACT I GODZUA CORNÉLIO RODRIGUES I CEO

+244 222 789 201 - 938 769 108(131)

admin@operacoes-gcr.com