ANTI-FRAUD POLICY

Oceana Group Limited

Oceana House
25 Jan Smuts Street
Foreshore
8001

POLICY NAME	ANTI-FRAUD POLICY			POLICY NO.	1
EFFECTIVE DATE	23 November 2021	DATE OF LAST REVISION	2 August 2023	VERSION NO.	5

POLICY OWNER	Jayesh Jaga	CONTACT INFORMATION	Jayesh.jaga@oceana.co.za

APPLIES TO					
BOARD MEMBERS	X	EXCO	X	PERMANENT EMPLOYEES	X
TEMPORARY EMPLOYEES	X	VISITORS	X	CONTRACTORS	X

SUMMARY OF CHANGES TO CURRENT REVISION:

NO.	DESCRIPTION OF CHANGES
5	Policy owner change and name change. Insertion of financial reporting thresholds and update definition of theft.

DOCUMENT APPROVAL LIST:

NAME	POSITION	SIGNATURE	DATE
Jayesh Jaga	Chief ESG Officer and CoSec		05/09/2023
Neville Brink	Chief Executive Officer		05.09.2023
Nomahlubi Simamane	Chairperson: Social, Ethics and Transformation Committee		05.09.2023
Mustaq Brey	Chairman of the Board		05.09.2023

INTRODUCTION

The Oceana Group has a commitment to the highest legal, ethical and moral standards. All employees, agents, customers, suppliers and contractors are expected to share this commitment. The Fraud Prevention policy has been established to facilitate the development of reporting procedures which will aid in the prevention, detection and investigation of fraud and related offences (i.e. theft or corruption).

At Oceana, we aim to create a culture of fraud awareness to reduce the likelihood of fraud occurring and to encourage fraud reporting.

PURPOSE

This policy is designed to – foster a culture of business ethics within the Group; clearly communicate standards of ethical business practice for the Group and its employees; clarify acts considered to be fraudulent, to assist and guide managers in finding ways to minimise the risk of fraud; ensure a uniform approach to compliance with laws and established principles; reinforce a zero-tolerance approach to unethical and fraudulent conduct; establish procedures for reporting and dealing with unethical and fraudulent conduct; encourage managers to implement effective controls against fraud; and reduce exposure to fraud, theft and corruption.

SCOPE

This policy applies to the entire Group, including its subsidiaries and/or division, employees, agents, customers, suppliers and contractors. The Group encourages a high level of awareness of the policy amongst all employees and will continue to assess risk and provide guidance regarding procedures to be followed when unethical or fraudulent conduct is suspected.

POLICY STATEMENT

The Oceana Group is committed to: -

1. Introducing appropriate measures to assess and minimise the risk of fraud, i.e. technology, processes, systems, training, and awareness;
2. Providing appropriate mechanisms for employees to report suspected unethical and fraudulent behaviour and protecting those who do so;
3. Investigating all allegations of unethical conduct, fraud or corruption;
4. Taking appropriate action when unethical conduct, fraud or corruption is proved;
5. Proactively monitor fraud alerts provided by local, national and global authoritative bodies and update staff promptly; and
6. Ensuring that the requirements of the applicable legislation are complied with, particularly in respect of reporting certain offences.
7. Creating and nurturing a culture of ethical conduct in managing resources of the company and intolerance to fraud, corruption and financial misconduct
8. Taking appropriate action, including criminal action, against any person who attempts to or assists with committing fraud, corruption and other criminal activity

The Group will not offer, pay or accept bribes in its dealings in the marketplace and will not tolerate any such activity by any of its employees.

TERMS AND DEFINITIONS

TERM	DEFINITION
Oceana or Group	Oceana Group Limited, its divisions and/or subsidiaries.
Company	Oceana Group, a division and/or subsidiary within the Group.
Company Rules	Includes the company policies, codes, procedures etc.
Employees	All people working for or providing services to or within the Group, including officers, employees, independent contractors and agents (irrespective of their employment status within the Group).
Premises	Includes any Company building, vehicle, fishing vessels

REQUIREMENTS

1. **Measures to Minimise the Risk of Fraud**
   In order to maintain the Group's high standards, procedures and controls have been established to provide an environment which will minimise the opportunity for fraud. These procedures and controls help the Group conduct its business in an ethical manner. They establish the rules to which employees must adhere to and which have been prepared for the key functions of the Group.

   Particular attention is paid to the application of effective fraud prevention controls in:
   - new customer or supplier screening, conflict of interest checks and other checks;
   - accounts payable and reconciliation activities, including management of payees, interactions with the organisation's bank(s) and secure use of online/mobile banking and payment facilities;
   - ensuring the integrity of employees, especially those employed in customer or supplier screening, financial duties and information technology (where technical access levels raise fraud risk), with thorough background checks, monitoring of ongoing duties and work, and annual leave trends;
   - the use of information technology including secure email, file transfer and protection against a range of cyber threats.

2. **Guidelines to Identify Fraud/Unethical Conduct**
   All frauds involve an intentional and unlawful misrepresentation to the detriment of the business. The list below is not necessarily exhaustive but is intended to provide examples of what is considered fraudulent or unethical.

   There are generally the following broad categories of fraud:

   2.1. The definition of theft for this policy is the misappropriation of cash or assets to which, *inter alia*, the employee, external

contractors, visitors, suppliers, unknown third parties are not entitled. Theft of business assets includes, amongst others, theft of: -stock (shrinkage); computer equipment; intellectual property (includes customer lists, price lists or trademarks); funds through electronic banking false expense claims; and payroll fraud.

2.2. False accounting, which includes falsifying the results of the business.
2.3. Creating any false documentation or false entries on documentation.
2.4. Unlawfulness in the handling or reporting of monetary transactions.
2.5. Authorising or receiving payment for goods not received or services not rendered.
2.6. Receipt of kickbacks or commission from a supplier as a reward for being awarded a contract.
2.7. Soliciting kickbacks or commission from a supplier as a reward for being awarded a contract.
2.8. Authorising or receiving payment for hours not worked.
2.9. Claiming paid leave (e.g. sick leave) under false pretenses.
2.10. Misrepresentation of information on documents, including references.
2.11. Forgery or alteration of documents.
2.12. Transgression of the Group Code of Business Conduct and Ethics.

3. Defalcation Reporting Procedure

The Group requires suspected fraud or any irregular activity to be referred to the personnel mentioned in paragraph b below. Furthermore, the Group acknowledges that employees are vital to the successful implementation of measures against fraud and as a result, employees are encouraged to report any concerns they have, without fear of being penalized. The reporting of fraud/theft should be documented and reported according to the thresholds below:

Threshold	Authority to report fraud/theft to
< R100 000 (Less than One hundred Thousand Rand)	Chief Ethics Officer and CEO
> R100 000 (More than One hundred Thousand Rand)	Police/ Hawks/ appropriate authority (per the Prevention and Combatting of Corrupt Activities Act, Actb12 of 2004)
> R 1 000 000 (One Million Rand)	Audit Committee and SETCOM
Misappropriation or theft that could have a reputational impact on the business (regardless of financial value)	Audit Committee and SETCOM

The following routes are available to all employees, to freely voice concerns with any of the following personnel: Line Managers; Divisional Managing Directors; Executive: Sustainability & Compliance; Group Executive: Compliance and Risk; Group Chief Financial Officer; Group Chief Executive Officer; or Whistleblowers, an outsourced and independent call centre, which enables employees to report any instances of unethical or fraudulent behaviour. The below toll-free numbers are available for purposes of reporting any known or suspect inappropriate practices.

No.	Region	Toll-free Number
1.	South Africa	0800 00 66 60
2.	Namibia	0800 000 666
3.	United States	800-813-5990

All concerns reported will be treated in confidence and fully investigated. If anonymity is requested, every effort will be made to ensure such confidentiality. Employees should be aware that, if a suspicion is reported and results in a prosecution or disciplinary hearing, their involvement as a witness in those processes may be necessary, unless other substantial reliable evidence is available.

There is also a need to ensure that the investigative process is not misused. Therefore, any abuse, such as raising unfounded or malicious allegations, may be dealt with as a disciplinary matter. This should not deter employees from raising genuine concerns (even if subsequently unfounded but made with good intent), as, in so doing, they will be supported in every possible way.

4. Investigation Procedure

All reported suspected unethical or fraudulent incidents will be thoroughly investigated. The initial investigation should be conducted by a management task team appointed by the Divisional Managing Director, including the Executive: Sustainability & Compliance. If considered necessary, in the discretion of the Divisional Managing Director and the Chief ESG Officer, external consultants such as forensic accountants or professional investigators may be instructed to assist in the investigation.

5. Audit and Review

The Group employs rigorous audits and reviews (both internal and external) to monitor compliance with regulations and our own procedures, and undertakes a rolling programme of checks to detect, deter and prevent fraud and corruption. Monitoring systems and procedures are used to ensure that fraud prevention procedures are observed and remain appropriate and practical.

6. Staff Training, Monitoring and Detecting Fraud

Staff provide the best protection against fraud and corruption. It is important, therefore, that the policy on fraud prevention is fully communicated to all staff. The lack of clear guidance and ignorance of procedures will often be the first excuse used by offenders. Staff awareness of policy and procedures is fundamental to the effective operation of systems. In addition, all employees must be reminded, at least annually, of the monitoring, detection and reporting technologies and processes which employees are required to use.

7. Disciplinary proceedings

7.1. The terms and conditions of this policy have the force and effect of Company Rules. Contraventions of this policy will expose the employee to disciplinary action in accordance with the Company's Rules and Disciplinary Code, as amended from time to time.

7.2. Contraventions of this policy may require that criminal charges are laid with the police services in the regions in which we operate (incl. South Africa, United States of America, and Namibia) against the employee, and/or the company may decide in any event to lay a charge that could result in criminal prosecution.

MANAGEMENT ROUTINES

1. This policy is published on the Group's intranet portal for all employees to access and read.
2. The divisions and/or subsidiaries of the Group must publish this policy or a divisional policy that is aligned to this policy on notice boards or designated communication areas for employees who do not have access to computers.
3. The policy is reviewed every 2 years but may be reviewed more often depending on best practice and changes to our business, technologies or regulatory environment.

LEGISLATION

The following laws and principles either require us to comply with them or may be relevant in determining this policy.

South Africa

- Constitution of the Republic of South Africa, 1996
- Prevention and Combating of Corrupt Activities Act, 2004
- Prevention of Organised Crime Act, 1998
- Financial Intelligence Centre Act, 2001
- Protected Disclosures Act, 2000
- Companies Act, 2008
- Competition Act, 1998

United States of America

- Constitution of the United States of America, 1787
- Foreign Corrupt Practices Act,1977
- Corporate Governance Law
- Antitrust and Competition Law
- Louisiana Unfair Trade Practices and Consumer Protection Law
- Whistleblower Statute

Namibia

- Constitution of the Republic of Namibia, 1990
- Anti-Corruption Act, 2003
- Prevention of Organised Crime Act, 2004
- Financial Intelligence Act, 2012
- Whistleblower Protection Act, 2017
- Companies Act, 2004
- Competition Act, 2003

This is not an exhaustive list, as other laws, regulations, standards and codes of practices may also be relevant.

RELATED POLICIES AND OTHER REFERENCES

Related policies

1. Anti-Bribery and Corruption Policy
2. Code of Business Conduct and Ethics
3. Compliance Policy
4. Risk Management Policy
5. Disciplinary Code
6. Speak-Up Policy

This is not an exhaustive list, as other policies, processes and procedures may also be relevant.

ROLES AND RESPONSIBILITIES

List the job titles and business offices directly responsible for policy.

ROLE	RESPONSIBILITY
Managers	Managers must establish monitoring systems and procedures designed to detect and avoid fraudulent or related dishonest activities in their respective areas of responsibility and particularly in business areas that are identified as vulnerable / at risk. The relevant Managers must ensure and implement effective controls against fraud, including: • reference checking during recruitment process; • operating effective access controls within premises; • procedures for awarding contracts for the supply of goods and services e.g. transporting of products; • internal audit checks, which include risk-based audits of operational aspects; • an adequate separation of duties (more than one employee being involved in key tasks where fraud might occur); • proper authorisation procedures (transactions being approved appropriately regardless of hierarchy); • independent monitoring and checking of data and documentation (checks and balances) • a full understanding and communication to employees of secure practices when making payments.
Line Managers	Line Managers must implement and ensure proper application of this policy and the associated procedures.
Employees	Employees must report any suspicions of fraud or any irregular activity and may do so without fear of reprisal.

CONTACTS

List contacts in the table.

SUBJECT	CONTACT	PHONE	EMAIL
Executive: Compliance and Sustainability	Karen-Dawn Koen	021 410 1475 082 044 5400	Karendawn.Koen@oceana.co.za
Chief ESG Officer	Jayesh Jaga	021 410 1411 082 495 4225	Jayesh.Jaga@oceana.co.za

VERSION HISTORY

VERSION	APPROVED BY	REVISION DATE	DESCRIPTION OF CHANGE	AUTHOR
4	Jillian Marais	1 September 2021	New format and update	Nabeelah Edwards
5	Jayesh Jaga	2 August 2023	Name change and policy owner change. Insertion of financial reporting thresholds and update definition of theft.	Nabeelah Sawant

LEGAL COMMENTS

None

ADDITIONAL NOTES

None