

WORLDWIDE ADVISORY SERVICES (PTY) LTD

(Hereinafter referred to as 'the Company')

ANTI-BRIBERY, CORRUPTION & MONEY LAUNDERING POLICY



Worldwide
Advisory Services

DOCUMENT MANAGEMENT	
Title: WWAS Anti-bribery, Corruption & Money Laundering Policy	
Implementation Date: July 2025	
Version Status: Version 1.0	
Last Review Date:	
Next Review Date: July 2026	

VERSION AND APPROVAL CONTROL				
Version	Type	Summary of actions/changes	Responsible Party	Date
V 1.0	New	New document produced	WWAS Legal & Compliance Manager – Byron Bosch	July 2025
V 1.0	Approval	Approved	WWAS Director – Adrian Koekemoer	July 2025
V 1.0	Approval	Approved	WWAS Key Individual – Liese Lindeque	July 2025

Version Type:

☐
New/Draft/Replacement
☐
Review (Annual/Ad Hoc)
☐
Amendment
☒
Approved

Contents

1. Introduction	4
2. What is Bribery, Corruption & Money Laundering?	5
3. Who is a Government Official?	5
4. What is the Law?	6
5. Bribery, Corruption & Money Laundering Prevention	7
6. Typical Bribery, Corruption & Money Laundering Risks	10

Annexure A

DN Invest Proprietary Limited and each of its subsidiaries (each a "**Company**" and collectively, the "**DNI Group**") subscribe to a Code of Ethics. In accordance with the principles set out in the Code, the DNI Group has produced this Policy designed to counter bribery, corruption and money laundering within its operations. Furthermore, DNI Group is committed to preventing corrupt activities conducted by its employees and any Associated Persons performing services for or on its behalf, consistent with the requirements of Section 34A of the Prevention and Combating of Corrupt Activities Act, 2004 ("**the Act**").

1. Introduction

This anti bribery, corruption and money laundering policy ("**Policy**") is applicable to:

- All employees of the DNI Group, including those individuals based at off-site workplaces;
- Any individual or entity acting on behalf of or under the control of the DNI Group, such as agents, intermediaries, representatives, distributors, consultants, business partners or joint venture partners ("**Third Parties**");
- Any individual or entity that performs services for the DNI Group ("**Service Provider**"); and
- Any other persons associated with the DNI Group (including any person performing services for or on behalf of DNI Group, irrespective of capacity, as defined under the Act Section 34A(2).
- Associated Persons: For the purposes of this Policy and in line with the Act Section 34A(2), a person is associated with DNI Group if, disregarding any gratification under consideration, that person performs services for or on behalf of DNI Group, irrespective of the capacity in which such person performs services. This includes, but is not limited to, employees, agents, contractors, consultants, suppliers, intermediaries, and joint venture partners.

The DNI Group has a zero-tolerance policy on theft, bribery, corruption, and inducements. It is committed to the highest levels of honesty, integrity, fairness, dignity, respect, transparency and accountability. The purpose of this Policy is to:

- Provide information and guidance to our employees, Third Parties, Service Providers and other Associated Persons on how to identify and avoid situations that could potentially violate anti- bribery, corruption and money laundering laws; and
- Set out the standards and procedures that the DNI Group has adopted in order to ensure that all persons associated with the DNI Group do not engage in any form of corrupt behaviour.

All persons associated with the DNI Group must be familiar with the rules described in this Policy and regularly refresh their understanding of these rules. If this Policy does not give you enough guidance on how to proceed in a particular situation:

- Employees must consult their line manager, their Company's Executives or the Company or Group Human Resources Department.
- Third Parties, Service Providers and other Associated Persons must consult their point of contact (i.e., contact person) based at the relevant Company.

Bribery, corruption and money laundering is illegal and can expose the DNI Group and persons associated with it to fines and other penalties, including imprisonment. Bribery, corruption and money laundering is also against the values of the DNI Group. For these reasons, compliance with this Policy is mandatory for the DNI Group and all persons associated with it.

It is important to note that a breach of this Policy will lead to disciplinary action against employees, and legal action, civil and/or criminal, may be taken against offenders (including employees).

The DNI Group is committed to ensuring that it is not involved, in any manner whatsoever, in unethical or corrupt activities. In particular, under no circumstances may any employees, Third Parties, Service Providers or any persons associated with the DNI Group give or agree, or offer to give any gratification prohibited in terms of Chapter 2 of the Act to another person, including to obtain or retain:

- Business for the DNI Group; or

- An advantage in the conduct or business for the DNI Group.

Chapter 2 of the Act regulates the general offence of corruption and offences in respect of corrupt activities relating to public officers, foreign public officials, agents, members of legislative authority, judicial officers and members of the prosecuting authority.

Below, the following sections of this Policy address the following:

- **Sections 2 to 4 of the Act** explain the concepts of bribery, corruption, and money laundering and provide insight into the legal position on these concepts in South Africa.
- **Section 5 of the Act** explains the steps that must be taken to prevent bribery, corruption and money laundering – these are referred to as the "six principles".
- **Section 6 of the Act** explains the categories of risk where bribery, corruption and money laundering typically arise, and the DNI Group's position on each category of risk.

2. What is Bribery, Corruption & Money Laundering?

A bribe is an inducement or reward offered, promised, or provided in order to gain any commercial, contractual, regulatory or personal advantage.

Corruption is the misuse of public office or power for private gain or the misuse of private power in relation to business outside the realm of government.

Corruption includes bribery, theft, extortion (i.e. taking from another some advantage by subjecting that person to pressure which induces him or her to submit), fraud and the misuse of company assets. It also includes any activity which constitutes an offence in terms of section 64 of the Financial Intelligence Centre Act, 2001 or sections 4,5, or 6 of the Act. A conflict of interest has the potential for corrupt conduct, when an individual or corporation takes advantage of the conflict of interest and abuses their position for private gain.

Money laundering means an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds.

Acts of bribery or corruption are intended to influence an individual in the performance of their work to act dishonestly and/or improperly. The person being bribed is usually someone who can obtain, retain or direct business, for example, during a tender or contracting process or it may be through the handling of administrative tasks or customs matters.

A bribe can take many forms. For example, a direct or indirect promise or offer of something of value, the offer or receipt of a kickback, fee, reward or other advantage, the giving of aid, donations or voting designed to exert improper influence.

Those engaged in bribery, corruption and money laundering can include an employee, officer, director and/or any person who performs services for or on behalf of an institute, i.e. agents, individuals, organisations who authorise someone else to carry out these acts and/or government or public officials, whether foreign or domestic.

3. Who is a Government Official?

A government official includes anyone, regardless of rank, who is:

- An officer or employee of any local, provincial or national government (for example, members of parliament, police officers, firefighters, members of the military, tax authorities, customs or health inspectors, etc.);
- Any person acting in an official capacity or on behalf of any government or public international organisation (for example, an official advisor to a government);
- Any officer or employee of a political party;
- Any candidate for political office;
- A close relative of any of the above (for example, parent, sibling, spouse or child);
- A director, officer, representative, agent or employee of any government-owned or controlled business or group (meaning that the government owns some shareholding of the stock or business, or is its largest shareholder, or controls the entity through its management, board membership or other means); or
- An officer or employee of a public international organisation (for example, the United Nations, International Olympic Committee, International Red Cross, World Health Organisation, etc.).

The DNI Group does not condone bribing and unjustly influencing government officials. When meeting with government officials, at least two representatives from the relevant Company should be present and the government officials should be informed that the meeting may be recorded.

4. What is the Law?

In South Africa, bribery, corruption and money laundering are regulated by the Act. It is important to note that penalties for a contravention of the Act include a life sentence, demonstrating the importance that the law attaches to combating corruption. The crime of corruption is set out in the Act as follows –

‘Any person who, directly or indirectly:-

- (a) 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
- (b) 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, in order to act, personally or by influencing another person so to act, in a manner:
 - (i) That amounts to the:
 - (aa) illegal, dishonest, unauthorised, incomplete, or biased; or
 - (bb) misuse or selling of information or material acquired in the course of the exercise, carrying out or performance of any powers, duties or functions arising out of a constitutional, statutory, contractual or any other legal obligation;
 - (ii) That amounts to:
 - (aa) the abuse of a position of authority;
 - (bb) a breach of trust; or
 - (cc) the violation of a legal duty or a set of rules,
 - (iii) Designed to achieve an unjustified result; or
 - (iv) That amounts to any other unauthorised or improper inducement to do or not to do anything, is guilty of the offence of corruption.’

It is also important to understand that the Act clearly states that any member of the private sector (which includes any Company within the DNI Group) is guilty of an offence if someone associated with them gives or agrees or offers to give any gratification prohibited in terms of Chapter 2 of the Act to another person. This offer or gift is made or given with the intent to obtain or retain business for that member or to gain an advantage in that member's business operations. An individual or entity is considered associated with a private sector member if they perform services for or on behalf of that member, regardless of their role or capacity.

The penalties that may be imposed for a contravention of the Act range from 5 years to life imprisonment. It is also important to note that the Act includes certain provisions that assist with the prosecution process.

In addition, any person who holds a position of authority and who knows or ought reasonably to have known or suspected that any other person has committed an offence in terms of sections 3 to 16 or 20 to 21 of the Act or the offence of theft, fraud, extortion, forgery or uttering a forged document, involving an amount of R100 000.00 or more, must report such knowledge or suspicion or cause such knowledge or suspicion to be reported to a police official in the Directorate for Priority Crime Investigation referred to in section 17C of the South African Police Service Act, 1995. Any person who fails to report is guilty of an offence.

Money laundering is governed by the Financial Intelligence Centre Act, 2001 as amended by the Financial Intelligence Centre Amendment Act, 2017 and associated regulations and guidance notes as well as the Prevention of Organised Crime Act, 1998.

5. Bribery, Corruption & Money Laundering Prevention

The prevention of bribery, corruption and money laundering includes the following steps:

1. Principle 1: Top Level Commitment: The DN Invest Board and each Company's Executives and senior management team are fully committed to preventing and detecting bribery, corruption and money laundering. This commitment is demonstrated by:
 - Implementing and maintaining this Policy.
 - Providing adequate resources for training and compliance.
 - Providing an independent Fraud and Ethics Hotline and other channels to report unethical or criminal conduct.
 - Leading by example and promoting a culture of ethical behaviour.
 - General oversight of breaches and assurance as provided by the Group's Head Office Executives during the DN Invest Board and Committee meetings.
2. Principles 2 and 3: Risk Assessment and Proportionate Procedures:
 - Each Company is required to undertake periodic risk assessments in order to identify the areas in which it faces higher risks of bribery, corruption and money laundering (i.e., the vulnerable areas). This includes identifying and assessing where these risks may arise in respect of its business activities, clients, service providers, products and/or services and geographic locations. These risk assessments must be informed and documented.
 - Each Company must seek to allocate adequate resources and implement appropriate processes based on the level of risk to effectively mitigate and manage the risk of bribery, corruption and money laundering (i.e., implement proportionate procedures based on the identified risks). These procedures may include Know Your Client (KYC) checks, enhanced due diligence, transaction

monitoring, record keeping and the implementation of prevention mechanisms related to the areas identified as high risk. By identifying the high-risk areas, each Company is able to take steps to mitigate the risks.

- Relevant factors to consider for proportionate procedures may include: (i) size of the organisation; (ii) nature of the industry; (iii) jurisdiction where the organisation operates; (iv) use of third parties; and (v) organisation structure.

3. Principle 4: Due Diligence:

- Before entering into relationships with employees, Service Providers or Third Parties, each Company should conduct a due diligence to assess their integrity, reputation, and risk of involvement in bribery, corruption and/or money laundering. The level of perceived risk should inform the nature of the due diligence to be conducted.
- It is highly recommended that a Company conducts an enhanced due diligence for high-risk entities or transactions and for employees occupying high risk positions.
- The following are considered HIGH RISK:
 - (i) A multi-layered entity without any apparent and commercially logical reason for the complexity of the structure.
 - (ii) Entities or employees with close relations to a:
 - (aa) Domestic politically exposed person, being any person who holds, including in an acting position, for a period exceeding six months, or has held a prominent public function in the Republic of South Africa (or any other country within which the DNI Group operates).
 - (bb) Foreign politically exposed person, being any person who holds (or has held) in any foreign country, a prominent public function.
 - (cc) Prominent influential person, being any person who holds or has held within the preceding 12 months, the position of Chairperson of the board of directors; Chairperson of the audit committee; Executive officer; or Chief Financial Officer in a company providing goods or services to an organ of state.
 - (iii) Entities that deal with dual-use goods, being products, technologies, or materials that have both civilian and military applications.
 - (iv) Cash payment/s to the value of R50,000 or higher.
 - (v) Demands, without any logical reason, for the immediate transfer of funds.
 - (vi) The value of the transaction exceeds what one would expect to be affordable for a client.
 - (vii) Unwarranted/unexplained international transfers without any reasonable explanation.
 - (viii) Entities that originate or operate from a Financial Action Task Force identified high-risk geographical jurisdiction (the exception being South Africa).
 - (ix) A partnership, trust, company, close corporation, or other legal entity, regardless of whether or not it was formed in South Africa, which has no operations or business premises in South Africa.
 - (x) Where a transaction is considered suspect for any reason relating to the other party's conduct, which conduct may include (without limitation):
 - (aa) A reluctance or refusal to provide information, or deliberate evasiveness or vagueness when providing information;

- (bb) An unusual or inexplicable preference for dealing with the Company via correspondence or via electronic media, as opposed to in person, particularly for the purposes of the due diligence;
 - (cc) Reversing of transactions before repayments of a loan has started, resulting in the borrowed funds being repaid within a short space of time;
 - (dd) Repayment amounts for loans are higher or within a shorter time frame than originally agreed upon with no reasonable explanation for this or the source of funds used;
 - (ee) Multiple cash repayments without a plausible explanation for the source of funds;
 - (ff) Multiple loans are taken out which do not make sense or do not fit the economic profile of the client;
 - (gg) A change in the business or the business strategy of the borrower that does not make economic sense;
 - (hh) A loan is serviced by a third party that was not part of the original transaction; and
 - (ii) Any other conduct or circumstances that, when viewed objectively, and when considered in light of all of the relevant factors taken as a whole, should be regarded with suspicion.
 - (xi) Information is provided that cannot be verified and there is no logical reason that it cannot be verified.
 - (xii) Executives, directors, and other senior management personnel who have significant control over financial decisions and transactions.
 - (xiii) Employees who have access to financial systems or are involved in processing payments and transactions.
4. Principle 5: Communication, Education and Training – Each Company must seek to:
- Communicate this Policy to all persons associated with it;
 - Ensure that this Policy and the WWAS Code of Ethics are reviewed and understood by employees;
 - Conduct ongoing and effective education and training on how to comply with this Policy and the WWAS Code of Ethics; and
 - Remind persons associated with it to report any suspected violations of this Policy to their line manager or contact person or the Group Fraud and Ethics Hotline or the relevant communication channel.
5. Principle 6: Effective Monitoring and Internal Controls
- Each Company must maintain an effective system of internal anti-money laundering, corruption and bribery controls and monitoring of these controls to help mitigate the risks of money laundering, corruption and bribery on an ongoing basis.
 - In particular, each Company must at least have the following procedures in place to monitor its anti-money laundering, corruption and bribery controls:
 - (i) Regularly reviewing its risk assessment and procedures.
 - (ii) Monitoring transactions for suspicious activity, with due regard to the high-risk factors listed above.
 - (iii) Investigating any suspected violations of this Policy.
 - (iv) Taking appropriate disciplinary action against any employees who violate this Policy.
 - (v) Taking appropriate legal action against any individual and/or entity who violates this Policy.
 - Each Company must ensure that it retains accurate books, records and financial reporting. Bribery, corruption and money laundering are typically linked to poor record-keeping.

6. Typical Bribery, Corruption & Money Laundering Risks

Bribery, corruption and money laundering risks typically fall within the following categories:–

Gifts, entertainment and hospitality

Unacceptable Business Courtesies: In order to provide specific guidelines to employees, the following acts, amongst others, are deemed unacceptable:

- Acceptance of gifts or any considerations which would be perceived as having a value to the recipient, for example, sponsored holidays, hunting trips, flight tickets for personal use, jewelry, electronic equipment, any other luxury items etc. Offers of this kind must be firmly declined or immediately returned to the sender if delivered without prior notice, unless approved by an Executive or director of the relevant Company and where refusal would unnecessarily offend the donor.
- Acceptance of cash payments, whether large or small, must be refused under any circumstance.
- Airline tickets and/or accommodation for business trips or trips for training or study purposes, paid for by the third party are not considered as prohibited if approved by the relevant managing director/CEO.

Doing Business with the Public Sector

- There is an absolute prohibition on the DNI Group and/or its employees providing any benefit of whatsoever nature, directly or indirectly, to any employee in the public sector. Any business conducted with the public sector will be performed on sound commercial terms.

Political, Charitable and other Public Activities and Business Affiliations

- In general, the DNI Group would not expect that a conflict of interest will arise from a director or employee's affiliation with outside professional, political, civic or charitable organisations or (subject to written approval by the DNI Group in advance) from directorships or trusteeships of non-competing business entities who do not trade with the DNI Group. Any request for such approval should be submitted in writing to the relevant Company's CEO. An employee should disclose any such activities where the employee has reason to believe that an invitation to serve in any such organisation was offered primarily because of the person's employment with the DNI Group or where there is an implication of DNI Group's interest or responsibility.
- In order to avoid such an inference, an employee shall not use the Company or its premises for charitable, political or other purposes outside the employee's normal duties and responsibilities.

Charitable Donations

- Overall limits for charitable donations by the DNI Group and/or individual Companies within the Group will be approved by the Board from time to time.
- To ensure that no donation can be misconstrued as a bribe, any donation given on behalf of any Company must comply with the following guidelines:
 - (i) any request for a donation must be made in writing and must sufficiently describe the charitable purpose of the donation, any business reason for the donation, and all details about the recipient;
 - (ii) the recipient must be screened to determine that it is a legitimate charitable organisation;
 - (iii) the donation must be approved in writing by the relevant Company Executive; and
 - (iv) the donation must be accurately recorded.
- All donations given must be recorded in the register maintained for this purpose on a monthly basis (see Annexure A) and declared on a quarterly basis. The completed register must be submitted to the Group's Chief Operations Officer and Compliance Office on a quarterly basis or when requested.

Facility Payments

- In many countries, it is customary business practice to make payments or gifts of small value to government officials in order to speed up or facilitate a routine action or process. Such payments are called "facilitating payments". Facilitation payments are a direct and serious violation of this Policy.
- Facilitation payments exclude payments which are made on market standard terms, such as channel fees to sales partners or profit-sharing arrangements to contract originators. These will be considered on an ad hoc basis on their merits and based on industry standards, guidelines and the Group's Code of Ethics.
- Examples of routine, non-discretionary actions include providing police protection, granting visas or utility services, or clearing customs.

Non-solicitation

- No director, supplier, customer, contractor, joint venture partner or employee of the DNI Group is to make, offer, promise or authorise an unlawful or improper payment of any kind, whilst knowing that such payment is intended as a bribe, payoff or rebate in an attempt to coerce any individual into awarding business opportunities to the DNI Group or preventing any business opportunity from being denied to or withdrawn from the DNI Group. This view on non-solicitation should be clearly communicated to all parties that conduct business with the DNI Group.
- Individuals are warned that such conduct could have serious consequences for the DNI Group and the individual concerned, including but not limited to, criminal and civil prosecution and the DNI Group will investigate and pursue any such allegations to the full extent of the law.

Relationships with Governments

- The DNI Group respects the authority of the governments in the countries in which it conducts its business. It is therefore imperative that directors and employees maintain an honest, transparent and ethical relationship with the government, their agencies, officials and personnel.
- Directors and employees must ensure that when providing information relating to the DNI Group or a Company to representatives of the government, that the information is accurate, comprehensive and in compliance with applicable laws and regulations relating to corporate participation in public affairs.

Third Parties

- Bribery problems often involve third parties. For this reason, all Third Parties must comply with this Policy.
- Because anti-bribery laws prohibit "indirect" as well as direct payments and offers, the DNI Group and directors and employees of a Company may be held liable for the conduct of Third Parties when they know or reasonably should have known of any unlawful conduct. Turning a "blind eye" or ignoring "red flags" that something may be wrong does not exonerate a Company or an individual from criminal liability.
- Authorising a Third Party to do something that you cannot do directly is a violation of this Policy.
- A reasonable investigation should be conducted into a Third Party's background, reputation, and business capabilities prior to entering into any contract. This investigation is called a due diligence and should be documented.
- Compensation to Third Parties must be commercially reasonable and commensurate with the tasks that they actually undertake. Contracts should generally provide fixed compensation for specific, identified tasks and should avoid large percentage-based commissions and success fees.

- Payments to Third Parties must be made in accordance with the terms of the contract entered into and in line with the applicable authority framework. It is a violation of this Policy to honour requests by Third Parties to vary the terms of contracts. Contracts that provide for payments to parties other than the contracting party, or payments to countries other than where the entity of the contracting party operates, must be approved in advance by the relevant Company's CEO.

Reporting of Wrong-doing: Tip-offs

Employees:

- The DNI Group maintains a Fraud and Ethics Hotline ("**Hotline**"), which is independently managed by an external service provider ("**External Party**"). Employees may make disclosures relating to money laundering, bribery, corruption and/or other financial crimes through the Hotline on an anonymous, partially anonymous or confidential basis.
- Employees can contact the Hotline to lodge their report using the following channels:
 - ➔ By calling the Hotline on the following toll-free number: 080 022 2708
 - ➔ By email at dni@tip-offs.com; and
 - ➔ Online at www.tip-offs.com. This site is also cell phone friendly and allows one to easily upload photos, audio or documents from ones cell phone.
- An agent from the External Party will seek to obtain as much information as possible. **Thereafter**, s/he will compile a report.
- All reports shall be sent to designated people within the DNI Group. These designated people shall be the DNI Group's Compliance Officer and Chief Financial Officer. If the reports pertain to either of these designated people, the reports will be sent to the DNI Group's Legal Counsel.
- If a person wants to remain anonymous or partially anonymous, a report analyst from the External Party shall remove his or her identity from the report and send the report to the designated people within the Group.
- If the report relates to any of the designated people within the Group, the report will be sent to the Deputy Chairperson of the DNI Board, who is a non-executive director.
- After the person lodges a report with the Hotline, he or she will obtain a unique reference number for their personal records.
- To receive feedback, the person may contact the Hotline through the prescribed channels and provide his or her unique reference number.
- The nature and complexity of the reported concern will dictate the action taken by the DNI Group.

Other stakeholders (including persons associated with the DNI Group and members of the public):

- Other stakeholders may report their concerns directly to the DNI Group's Compliance Officer, Chief Financial Officer ("**CFO**") or Legal Counsel by contacting them by:
 - ➔ Email at tipoffs@dninvest.co.za; and/or
 - ➔ Telephone on 011 100 3800.
- If the concern pertains to any one or all of these individuals, stakeholders may report their concerns directly to the DNI Group's Board by e-mail at dni-tipoffs@sabvest.com. Stakeholders must not report concerns to the Board, unless it involves the DNI Group's Compliance Officer, CFO or Group Legal Counsel.

Related Laws (in alphabetical order)	
1	CIPC Guideline 1 of 2018
2	Financial Intelligence Centre Act 38 of 2001
3	Judicial Matters Amendment Act 15 of 2023
4	Organisation for Economic Co-operation and Development's publications concerning corruption
5	Prevention and Combating of Corrupt Activities Act 12 of 2004
6	Prevention of Organised Crime Act 121 of 1998
7	Protected Disclosures Act 26 of 2000
8	United Nations Global Compact Principles

Annexure A

Donations Register - (insert date) to (insert date)

The register below shows the nature and value of donations that have been given by the Company between (insert date) and (insert date).

The register is updated on a monthly basis.

Worldwide Advisory Services							
Donations given by the Company							
Details of recipient (confirmed that recipient is legitimate)	Name of Company Executive who approved donation in writing	Date of donation	S18A Certificate (Y/N)	Description of donation	The circumstances under which it was given (i.e. purpose, business reason etc.)	Donation amount or estimated market value of the donation	Utilised for BEE SED Spend (Y/N)