SAVANNAH ENERGY

Proud to partner Nigeria & Niger

Policy

Anti-Corruption and Anti-Money Laundering Policy and Procedures

Document Number: 2100000-SAVE-POL-CMP-0003
Date: 12/01/2022 **Revision:** 1

Approvals, Control and Amendment

An approval signature on the front cover indicates approval of this document. Controlled copies are identified by controlled status on front cover - only controlled copies will be automatically updated. Amendments to sections of this document are detailed in the following table. Approval of the amendment is indicated by the responsible Manager's initials on master soft copy and original signature on hard controlled copies.

Document history and change record

Issue	Issue date	Description of change
Rev 0	Jan-2020	Issued for use (IFU)
Rev 1	Jan-2022	Issued for use with minor comments incorporated (IFU)

Authorisation

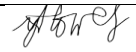
Role	Name	Title	Signature & Date
Prepared by:	Titilayo Okoye	Chief Compliance Officer	
Reviewed by:	Yasmin Howes	Legal Counsel	
Approved by:	Andrew Knott	Chief Executive Officer	

Table of Contents

1. INTRODUCTION 5
1.1 Statement of Company Policy 5
1.2 Applicable Laws 5
1.3 People to Whom this Policy Applies 6
1.4 Bribery Prevention Training 7
2. RESPONSIBILITY FOR COMPLIANCE 8
2.1 Chief Compliance Officer 8
2.2 Notification of Suspected Violations 8
2.3 Compliance Committees 8
2.4 Compliance Officer 8
2.5 Whistle Blower Protection 9
2.6 Anti-Corruption and Anti-Money Laundering Annual Compliance Questionnaire 9
2.7 Annual Compliance Review 10
2.8 Record Retention 10
2.9 Cooperation with Law Enforcement 11
3. ANTI-CORRUPTION POLICY AND PROCEDURES 12
3.1 Policy Regarding Travel Benefits, Gifts and Hospitality 12
3.2 Policy Regarding Benefits to Public Officials 13
3.3 Facilitation payments and kickbacks 14
3.4 Use of Company Assets and Accuracy of Financial Records 14
3.5 Prohibited Means of Payment 15
3.6 Charitable donations and political contributions 15
3.7 Doing Business Through Investments or Transactions with Business Partners 15
3.8 Further Guidance 15
4. ANTI-CORUPTION PROCEDURES REGARDING THIRD PARTIES 16
4.1 Background 16
4.2 Initial Business Justification and Third Party Identification (STEP I) 16
4.3 Due Diligence and Internal Risk Rating Process (STEP II) 18
4.4 Enhanced Diligence (Step III) 19
4.5 Contract Terms 21
4.6 Monitoring 21

4.7 Acquisitions of Businesses or Teams 22
4.8 Risk Assessment and Anti-Corruption Due Diligence 22
4.9 Local Legal Framework 22
5. ANTI-MONEY LAUNDERING POLICY 23
5.1 Background 23
5.2 What is Money Laundering? 23
6. ANTI-MONEY LAUNDERING PROCEDURES 25
6.1 Anti-Money Laundering Due Diligence 25
6.2 Detecting and Referring Suspicious Activity 26
7. SCHEDULE I OFFENCES UNDER THE BRIBERY ACTS 28
7.1 Penalty and Jurisdiction 28
8. GENERAL OFFENCES 28
9. FAILURE OF A COMMERCIAL ORGANISATION TO PREVENT BRIBERY 28
10. PAYMENTS TO FOREIGN PUBLIC OFFICIALS 29
SCHEDULE 1 CERTIFICATE COMPLIANCE 30
SCHEDULE 2 CERTIFICATE OF TRAINING 30

1. INTRODUCTION

1.1 Statement of Company Policy

Countries in which Savannah Energy Plc (the "**Company**") conducts business have adopted anti-corruption laws designed to combat the bribery, or other improper influence, of persons including, but not limited to, public officials. Anti-corruption laws typically include both anti-bribery prohibitions as well as financial record-keeping requirements. Anyone who breaks those laws can be subject to serious criminal and civil penalties including imprisonment, disgorgement of profits and asset forfeiture. Violations could also result in significant criminal and civil liability for the Company.

The Company operates on a zero-tolerance policy to bribery and corruption. It expects its employees and business partners to maintain the highest standards of ethical conduct and integrity and to comply with the letter and spirit of all applicable laws, regulations, treaties and conventions. Reference to the Company in this Policy shall, unless the context requires otherwise, be taken to refer to each subsidiary and affiliate of the Company (collectively, the "**Group**").

1.2 Applicable Laws

The Company has designed this Anti-Corruption and Anti-Money Laundering Policy and Procedures document (this "**Policy**") to ensure the Company is compliant with anti-corruption and anti-money laundering laws of the countries with jurisdiction over:

a) the Company's business; and

b) its directors, officers, employees (permanent, contractors and temporary) ("Savannah Staff") and any other individual who, or entity which, performs services for or on behalf of the Company (including intra group services such as HR and IT and third-party representatives acting on behalf of the Company), referred to in this Policy as "Service Providers" and, together with Savannah Staff, "Associated Persons".

As an ongoing process, the Group Chief Compliance Officer ("**Chief Compliance Officer**") shall identify all persons who qualify as Associated Persons of the Company. The Company shall provide a copy of this Policy to each member of Savannah Staff and to those Service Providers which are required to receive it by the terms of their engagement with the Company.

The applicable anti-corruption laws include:

a) measures which have been adopted to implement national and international conventions and guidelines, including the United Nations Convention Against Corruption ("UN

Convention"), the African Union Convention on Preventing and Combating Corruption, ("AU Convention"), the Criminal Law Convention Against Corruption of the Council of Europe ("Criminal Law Convention"), the Office of Economic Co-operation and Development Convention on Combating Bribery of Foreign Officials in International Business Transactions ("OECD Convention"):

b) the Financial Action Task Force ("FATF") 40 Recommendations and 9 Special Recommendations establishing globally accepted standards for anti-money laundering;
c) United Kingdom Bribery Act 2010 ("Bribery Act");
d) United Kingdom Proceeds of Crime Act 2002 ("POCA"); and
e) the trade sanctions and economic embargo programs enforced by the U.S. Office of Foreign Assets Control ("OFAC").

hereafter collectively, "**Applicable Laws**".

It is important to note that the Applicable Laws do not relate only to the bribery of public officials. Bribery of private citizens is illegal too. This Policy therefore applies to bribery of any person regardless of their capacity or status.

1.3 People to Whom this Policy Applies

All shall adhere to, implement and monitor the implementation of the terms of this Policy in their own right.

Strict compliance with the requirements of the Applicable Laws and this Policy is mandatory for all Savannah Staff and, if required by the terms of their engagement with the Company, Service Providers. All Savannah Staff and those Service Providers which are required to do so by the terms of their engagement with the Company must review and adhere to this Policy as a condition of their employment or engagement.

All Savannah Staff and those Service Providers which are required to do so under the terms of their engagement with the Company must provide a Certificate of Compliance in the form set out at Schedule 1. **Error! Reference source not found.** to the Group Financial Controller, certifying that they have read and understood, and that they agree to comply with, this Policy.

Any Associated Person who knowingly fosters illegal conduct, ignores suspicious circumstances or fails to comply with the Applicable Laws or this Policy and related procedures, will, in the case of officers or employees of the Company, be subject to discipline, including possible termination of employment

and may, in the case of Service Providers, be subject to contractual penalties including possible termination of their engagement.

1.4 Bribery Prevention Training

This Policy emphasises the Company's commitment to bribery prevention training, as prioritised and prescribed by the Company Directors and senior management.

General bribery prevention training is mandatory for all Savannah Staff. It shall take the form of education and awareness raising about the threats posed by bribery in general and in the oil and gas sector in particular, and the various ways it is being addressed by the Company.

More advanced training shall be provided to certain Savannah Staff, tailored to the specific risks associated with specific roles. Refresher training shall be provided from time to time as required and at least every twelve (12) months.

The Company shall also, where appropriate, provide advanced bribery prevention training and refresher training to Service Providers who represent a higher degree of risk from a corruption perspective. Where the Company does not train such Service Providers itself, it shall encourage the relevant Service Providers to conduct their own bribery prevention training.

All Savannah Staff and those Service Providers who receive bribery prevention training from the Company must provide a Certificate of Training in the form set out at Schedule 2. **Error! Reference source not found.** to the Chief Compliance Officer, certifying that they received bribery prevention training and the date of such training.

2. RESPONSIBILITY FOR COMPLIANCE

2.1 Chief Compliance Officer

Questions about this Policy should be directed to the Chief Compliance Officer.

The Chief Compliance Officer shall be responsible for overseeing the day-to-day implementation of this Policy, such as:

a) circulating on a regular basis, to those Associated Persons deemed appropriate, a request for information regarding any gifts and hospitality which such persons may have given or received from business contacts during the previous quarter; and

b) conducting risk assessments and the appropriate level of due diligence on third parties with whom the Company is proposing to enter into contracts.

The Chief Compliance Officer must request a determination from the Compliance Committee in all cases where a high risk of bribery has been identified.

2.2 Notification of Suspected Violations

Any suspected violation of the Applicable Laws or this Policy should be immediately brought to the attention of the Chief Compliance Officer, who can be reached by telephone on 020 3841 4962 and by e-mail at compliance.officer@savannah-Energy.com.

The Chief Compliance Officer together with the Compliance Committee shall take any further action deemed necessary and appropriate, including considering whether to engage legal counsel to conduct a confidential internal investigation. No further action should be taken by the Associated Person until a response is received from the Chief Compliance Officer.

2.3 Compliance Committees

Any issues that may arise in relation to this Policy shall initially be discussed by the Compliance Committee.

2.4 Compliance Officer

The Chief Compliance Officer shall:

a) provide assistance or make a determination (as appropriate) in respect of any matter referred to him or her by the Group Financial Controller;

b) investigate possible violations or legal issues relating to this Policy;

c) consult with legal counsel, as appropriate, to address enquiries regarding, or violations of, this Policy;

d) inform the Chief Executive Officer, Group Financial Controller and, as appropriate, the Board of Directors or Audit Committee of possible violations or legal issues;

e) make recommendations to the Chief Executive Officer and, as appropriate, the Board of Directors or Compliance Committee, as to appropriate action to take to address possible violations or legal issues; and

f) provide an annual compliance report to the Chief Executive Officer and, as appropriate, to the Board of Directors or *Compliance Committee* (See 'Annual Compliance Review' in Section 2.7).

2.5 Whistle Blower Protection

This Policy prohibits retaliation in any form against individuals who, in good faith, report concerns about possible violations.

The Company shall not retaliate, nor shall the Company permit any member of Savannah Staff to retaliate, against individuals who raise good faith reports of possible impropriety to management or the Chief Compliance Officer.

The Company encourages individuals to put their name to any reports they make. It may otherwise be difficult to conduct an investigation which is meaningful and fair to all concerned.

More detail in connection with Whistleblower protections is provided in the Company's full Whistleblowing Policy.

2.6 Anti-Corruption and Anti-Money Laundering Annual Compliance Questionnaire

All Savannah Staff and those Service Providers who are required to do so by the terms of their engagement with the Company must complete, sign and return an annual Anti-Corruption and Anti-Money Laundering Compliance Questionnaire (the "Questionnaire").

The Questionnaire shall be distributed by the Chief Compliance Officer in November of each year.

In the case of Savannah Staff:

a) the Group Chief Compliance Officer shall distribute the Questionnaire to team leaders within the Company;

b) each team leader shall be responsible for ensuring that the Questionnaire is sent to his team and filled out, signed and returned to him or her by all team members;

c) the team leader shall review the completed Questionnaires; and

d) the team leader shall confirm to the Chief Compliance Officer by 31 December of each year either that:

I. no issues have been raised in or by any of the Questionnaires; or

II. issues have been raised in or by in one or more Questionnaires, copies of which shall be sent by the team leader to the Group Financial Controller.

In the case of Service Providers who are required to complete and return the Questionnaire by the terms of their engagement with the Company:

a) the Group Chief Compliance Officer shall distribute the Questionnaire to its principal contact; and

b) Questionnaires must be completed and delivered to the Chief Compliance Officer by 31 December of each year.

The Chief Compliance Officer shall confirm to the Compliance Committee by 31 January of each year:

a) whether any person obliged to return a completed Questionnaire failed to do so; and

b) either that:

I. no issues have been raised in or by any of the Questionnaires; or

II. issues have been raised in one or more Questionnaires, copies of which shall be sent to the Chief Compliance Officer.

2.7 Annual Compliance Review

The Chief Compliance Officer shall conduct an annual review in order to determine whether this Policy is fully understood and is being complied with and properly implemented (the “Annual Compliance Review”).

The Annual Compliance Review shall be presented to the Chief Executive Officer and, as appropriate, to the Board of Directors or Audit Committee.

More frequent reviews may be warranted if an Annual Compliance Review reveals material issues of non-compliance or indications that this Policy has not been fully understood and/or implemented.

2.8 Record Retention

The Company shall maintain copies of all records and communications to document the implementation and operation of this Policy for as long as it considers appropriate and in compliance with applicable laws.

Records may take the form of memoranda, e-mails, audit reports or other information that documents the operation of this Policy. Confidential records shall not be disclosed other than as permitted or required by law.

2.9 Cooperation with Law Enforcement

The Company is committed to cooperating with law enforcement and governmental authorities in accordance with Applicable Laws and regulations, and with due consideration for the privacy of clients and transaction counterparties.

The Company may be served with legal process (for example, a subpoena) or receive a written or oral request for information from law enforcement or other governmental authorities in connection with investigations or inquiries that relate to potential corruption or money laundering.

Any member of Savannah Staff served with legal process or who receives a written or oral request for information from a governmental agency or regulatory authority must refer the matter immediately to, in the case of London, the Chief Executive Officer or the Chief Compliance Officer and/or the General Counsel and, elsewhere, to the Country Functional Head. Only those persons or their delegates are permitted to respond to legal process or other requests for information and to communicate with governmental authorities with respect to such inquiries.

3. ANTI-CORRUPTION POLICY AND PROCEDURES

3.1 Policy Regarding Travel Benefits, Gifts and Hospitality

Bona fide hospitality and promotional or other business expenditure which seeks to enhance the image of the Company, better present its operations, or establish cordial relations, is recognised as an established and important part of doing business.

It is not the intention of the Applicable Laws to criminalise such behaviour. However, it is clear that hospitality and promotional or other similar business expenditure can be employed as bribes.

In order to ensure compliance with the Applicable Laws it is necessary to consider, on a case-by-case basis, whether the intended recipient of a travel benefit, gift or hospitality may be induced, or feel obliged, to reciprocate by way of improperly performing his or her function.

This may be more likely if the travel benefit, gift or hospitality in question is disproportionately generous. If it is reasonable in the circumstances, it shall be more difficult to establish whether the Company, by giving it, intended to induce the recipient to perform his or her function improperly.

No travel benefit, gift or hospitality shall be given in exchange for a business benefit or any improper business advantage. Nor should it be given if it is intended to influence, or could be perceived as influencing, a business decision by the recipient.

Any gift must be in accordance with Applicable Laws and local laws, modest in value, promotional in nature, appropriate for the occasion and customary or ceremonial in nature. Where practicable, it is recommended that gifts bear the Company logo.

Cash gifts to business contacts are expressly prohibited, as are cash equivalents, such as gift vouchers.

An Associated Person may receive from his or her business contacts, or offer or give to a person who is not a public official, any gift or hospitality which does not exceed $50 in value for each individual gift or $250 in value per head for each hospitality event (not to exceed a total value of $2500 in any financial year). Any such gift giving shall be properly recorded in the corporate books and declared in writing to the Chief Compliance Officer upon request.

Associated Persons who wish to offer or give a gift or hospitality which does not fall within the above criteria must seek and obtain prior approval from the Chief Compliance Officer. Requests for approval from the Chief Compliance Officer should be made in writing and can be made by email to compliance.officer@savannah-Energy.com. Requests must include the following information:

a) date of the proposed hospitality/gift;

b) names of each provider(s) and each recipient(s) of the hospitality/gift;

c) the nature of the hospitality/gift (for example, 'wine tasting event at [x]');

d) the purpose of the hospitality/gift (for example, 'developing a business relationship with [x]');

e) the 'per head' spend on each non-Company recipient; and

f) confirmation that the offer or acceptance of the hospitality/gift is not intended to influence a decision-maker to award or obtain a business advantage improperly (for example that, as far as the person making the request is aware, there is no forthcoming pitch, tender, contract renewal or other formal decision process).

Any provision of gifts, travel or lodging must be properly recorded in the Gifts and Hospitality Register. Associated Persons shall not select the third parties to whom travel or lodging shall be provided, and shall confirm in writing with the selected third party's supervisor the nature and duration of the travel or lodging.

In no case shall Associated Persons pay for or reimburse the travel or lodging of the family or friends of the third party. The Company shall not fund or reimburse any 'side trips' for third parties.

3.2 Policy Regarding Benefits to Public Officials

The following issues arise in relation to the provision of travel benefits, per diems, gifts and hospitality to public officials. They are to be considered in addition to the matters set out in Section 3.1.

Associated Persons must not offer or give any travel benefit, per diem, gift or hospitality to any public official, except that:

a) gifts may be given to such persons on or around a recognised gift-giving period, so long as the gift-giving is properly recorded in the Gifts and Hospitality Register and the nature and value of the gift accords with local norms. For example, the giving of sheep and sugar during Ramadan is acceptable; or

b) a travel benefit, per diem, gift or hospitality may be given to such persons with the express prior written approval of the Group Chief Compliance Officer. The Chief Compliance Officer will consider matters including:

I. the nature and value of the travel benefit, per diem, gift or hospitality;

II. the circumstances of the occasion;

III. the legality of the provision of the travel benefit, per diem, gift or hospitality under Applicable Laws and local law;

IV. the frequency of travel benefits, per diems, gifts or hospitality to any particular public official; and

V. whether any travel which is at the invitation or request of the Company is for a bona fide business purpose or in the performance of a particular contract.

If the Chief Compliance Officer gives approval, the travel benefit, per diem, gift or hospitality must be properly recorded in the Gifts and Hospitality Register.

3.3 Facilitation payments and kickbacks

Facilitation payments are a form of bribery made for the purpose of expediting or facilitating the performance of a public official for a routine governmental action, and not to obtain or retain business or any improper business advantage. Facilitation payments tend to be demanded by low level officials to obtain a level of service which one would normally be entitled to.

Facilitation payments must not be paid. If, however, Associated Persons are faced with situations where there is a risk to their or a colleague's personal security or the security of his or her family and a facilitation payment is unavoidable, the following steps must be taken:

a) the amount must be kept to the minimum;

b) the payment must be recorded; and

c) the payment must be reported to the Chief Compliance Officer.

In such circumstances, the Chief Compliance Officer shall keep a record of all payments made and report these to the Compliance Committee, which shall evaluate the business risk and develop a strategy to minimise such payments in the future. Such a strategy may involve use of UK diplomatic channels or participation in locally active non-governmental organisations, so as to apply pressure on the authorities to take action to stop demands for facilitation payments.

3.4 Use of Company Assets and Accuracy of Financial Records

The Company requires that all financial transactions be accurately reflected in the Company's financial records and in accordance with generally accepted accounting principles.

The Company and all Savannah Staff, together with those Service Providers which are subject to such a prohibition under the terms of their engagement with the Company, are prohibited from maintaining undisclosed or unrecorded funds or assets established for any purpose. Examples of undisclosed or unrecorded funds or assets include, but are not limited to, the following:

a) numbered foreign bank accounts;

b) bank accounts containing Company funds but held in the names of individuals;

c) unrecorded petty cash or 'black box' funds; and

d) real and personal property held by a nominee.

3.5 Prohibited Means of Payment

Associated Persons may not make a payment to an individual, representative, consultant, distributor or other party unless an approved contract is in place. No payments shall be made in cash, to numbered accounts, to third-country accounts or to third-party accounts unless specifically authorised by the Group Financial Controller, who shall liaise with the Compliance Officer as appropriate. All payments must be supported by properly documented invoices.

Cheques may only be written to 'cash' or 'bearer' where the Company has received an invoice in respect of the relevant payment and a receipt from the payee. Such payment, together with copies of the relevant invoice and receipt, must be properly recorded in the corporate books.

3.6 Charitable donations and political contributions

Associated Persons are only permitted to utilise Company assets or resources for charitable donations or political contributions subject to the express authorisation of the Chief Compliance Officer who shall base any such approval on the law of the jurisdiction where the donation is to be made, considering the amount, timing, and means of the contribution. The Chief Compliance Officer shall maintain records of any such approvals in the Company files.

3.7 Doing Business Through Investments or Transactions with Business Partners

The Company requires that all investments and transactions involving its Business Partners be memorialised in writing and be pre-approved by a member of the Compliance Committee. Any proposed business transaction involving public officials or state-owned businesses shall be subject to heightened due diligence. This may include commissioning an investigation agency to provide a report on any intermediaries who shall be liaising with public officials on behalf of the Company.

3.8 Further Guidance

Enquiries concerning this Policy should be directed to the Chief Compliance Officer. For employees only: please consult the Questions and Answers set out in Schedule 4.

4. ANTI-CORUPTION PROCEDURES REGARDING THIRD PARTIES

4.1 Background

From time to time, the Company may deem it necessary, reasonable, or prudent to engage third parties to provide services to it.

Before the Company enters into contractual relations of any kind with any third party it shall, first, assess the risk of that person committing acts of bribery on its behalf and, secondly, conduct an appropriate level of due diligence on that person.

Third parties may only be engaged after completion of the processes and any relevant approvals have been granted as detailed in this Section 4.

4.2 Initial Business Justification and Third Party Identification (STEP I)

The Company must assess and document the legitimate business need and justification for engaging a new third party.

Prior to engaging a new third party, the relevant business unit shall categorise the third party by size of the contract as follows:

a) Tier 1 Counterparties: those where the total value of the proposed contract/engagement is reasonably anticipated to be less than US$5,000 in any twelve (12) month period; and

b) Tier 2 Counterparties: those where the total value of the proposed contract/engagement is reasonably anticipated to be in excess of US$5,000 in any twelve (12) month period.

The relevant business unit shall not be obliged to categorise any third party as described in Section 4 if the Chief Compliance Officer has decided that there is a low risk of the relevant third party committing acts of bribery on the Company's behalf after having conducted an appropriate level of due diligence. For example, the appropriate level of due diligence to be conducted by the Company shall be low when contracting for IT, catering or cleaning services, but should, at the minimum, involve an internet search for adverse reports to reflect the low risk of such service providers committing acts of bribery on the Company's behalf.

For any Tier 1 Counterparties, where both of the following statements are confirmed as correct:

a) the third party is not dealing with public officials on behalf of the Company; and

b) the third party is a corporate entity that is not a personal service company (that is, a company that provides the services of an individual and is owned and operated by that individual, such as a contractor selling his services through a limited company), then there is no requirement

to conduct anti-corruption due diligence. However, if there are any concerns in relation to an arrangement which falls within this exemption from the requirement to conduct anti-corruption due diligence from a money laundering perspective, then they should be raised with the Group Chief Compliance Officer as soon as possible.

For any Tier 1 Counterparties where one or both of the statements set out in Section a) and b) is not correct then such Tier 1 Counterparties shall be treated as Tier 2 Counterparties for the purposes of this Section 4.

For all Tier 2 Counterparties, the relevant business unit shall prepare a brief internal memorandum ("**Initial Assessment**") which shall be used to justify the business rationale for engaging with the third party.

The Initial Assessment shall describe all material, relevant information and include:

a) scope and timeline of the work to be undertaken;

b) legal name of the third party (and if a subsidiary, name of the main parent company and ownership percent) and key contact (if different);

c) anticipated total size of the contract to be awarded in local currency (and in US dollars equivalent), if any element of the compensation is linked to securing business for the Company, and length of the engagement;

d) the way in which the third party became known to the Company;

e) rationale behind the selection of the third party and summary of any selection process undertaken;

f) relevant experience of the third party and expected benefits of the engagement with the third party;

g) reporting lines and monitoring process for the third party by the Company;

h) whether the third party shall be given any authority to act on the Company's behalf; and

i) whether the third party shall be engaged to assist with any processes required by public officials (e.g. securing of visas, getting materials through customs etc.).

The Initial Assessment shall not be deemed to be approved until it has been signed-off by the Chief Compliance Officer. The Chief Compliance Officer shall not sign-off the Initial Assessment unless he or she is satisfied that there is appropriate justification for engaging the third party.

Following approval of the Initial Assessment, the relevant business unit will carry out the due diligence and internal risk rating process as summarised in Section 4.3 below.

The Company shall not be required to repeat the procedure set out in this Section 4 **Error! Reference source not found.** in relation to a third party if that party is an existing third party service provider applying for a substantially similar role in the future, unless:

a) the third party was originally assessed more than two years previously;

b) the third party was originally assessed as presenting a high risk from a bribery perspective; or

c) the Company is otherwise aware that the third party now presents an increased risk from a bribery perspective.

However, if there are any concerns in relation to an arrangement which falls within this exemption from the requirement to conduct anti-corruption due diligence from a money laundering perspective, then they should be raised with the Chief Compliance Officer as soon as possible.

4.3 Due Diligence and Internal Risk Rating Process (STEP II)

Before entering into a contractual relationship with a Tier 2 Counterparty, the Company shall follow the anti-corruption process set out in its Risk Assessment Procedures Document (as amended from time to time). This process is summarised in this Section 4.3.

Requests made as part of the due diligence process should involve direct communications with the third party, internet based research and, where appropriate, the use of a third party due diligence provider.

Any concerns regarding findings from the due diligence process (or otherwise) relating to a third party service provider shall be reported directly to the Chief Compliance Officer.

Please refer to Schedule 5 for example indicators of potential bribery risks.

Tier 2 Counterparties

For third parties categorised as Tier 2 Counterparties, the following information shall be ascertained:

a) legal name and contact details of the third party;

b) if the third party is an individual, his or her date of birth and employment status;

c) if the third party is a corporate entity, its registered address, details of its ownership structure and details of any party with an ownership interest of more than 2.5%;

d) bank account details (including full name and location of bank);

e) details relating to the proposed method for payments;

f) if a public official or any family relation of a public official has an ownership interest in the third party;

g) if a public official or any family relation of a public official recommended the third party to the Company;

h) if there are any sanctions or trade restrictions against the third party;

i) if the third party intends to utilise a particular employee or third party to carry out work on its behalf, and if so the relevant details;

j) a review of the third party's company brochures or website materials (if available);

k) a Google search for international and local press accounts to see if the third party has been in the press associated with an ethical or corruption scandal; and

l) a World Check search on the third party, being an individual, or key stakeholders if it is a corporate entity,

In respect of Tier 2 Counterparties whose shares are publicly traded on one or more of the following stock exchanges: (i) New York Stock Exchange, (ii) NASDAQ OMX, (iii) London Stock Exchange, (iv) Tokyo Stock Exchange, or (v) Shanghai Stock Exchange, only the information set out in Section 0 (a), (c), (g) - (l) needs to be ascertained.

Internal risk rating

An initial internal risk rating of 'Low", 'Medium' or 'High' shall be assigned to each third party based on the answers to the due diligence questions. If a third party is required to undergo "Enhanced Diligence" in accordance with Section 4 a final internal risk rating of 'Low', 'Medium' or 'High' shall be assigned to the third party based on the outcome of the Enhanced Diligence process. Guidance for the rating criteria can be found in Section 4.3.

Any third party assigned an initial internal risk rating of 'Low' shall be presented to the Group Chief Compliance Officer for approval to enter into a contractual arrangement with the third party service provider. Notwithstanding any such approval being granted, the Company shall be obligated to comply with its delegation of authority policy before entering into a contractual relationship with the third party.

Any third party assigned an initial internal risk rating of 'Medium' or 'High' shall be subject to a further level of Enhanced Diligence as set out below.

4.4 Enhanced Diligence (Step III)

Any third party which is assigned an initial internal risk rating of 'Medium' or 'High' shall be subject to a further set of Enhanced Diligence questions so that the Company can fully assess the suitability of the third party for the proposed work and identify any specific areas of risk.

The Enhanced Diligence questions shall be informed by the findings of the initial due diligence exercise carried out in accordance with Section 4.3 and as such, the questions will be tailored according to the areas of risks identified which may include, but shall not be limited to, requesting:

a) the full names and dates of birth of persons who have ownership interests in the third party of 2.5% and if considered appropriate, citizenship information and CVs;

b) details of how the third party is organised and confirmation that the third party has been validly incorporated and registered under local laws;

c) details of any parent companies or trusts;

d) details of the third party's business activities, key clients/contracts and geographical areas of operations;

e) if the third party has any past criminal convictions (especially in the areas of tax evasion or bribery); any bankruptcies; and any cases of civil litigation in which the third party has been a defendant;

f) audited financial statements or tax returns if available, or at least a financial reference in cases where there is any doubt as to the third party's ability and resources to provide the services in question; and

g) the following information, with supporting documentation:

    I. a reasonable number of business references (if applicable) so that the Company may have an independent account as to the third party's effectiveness, standing in the community and reputation for ethical business practices; and

    II. if financial statements or tax returns are unavailable or do not provide a complete picture, financial references from the third party's bank(s).

Following the Enhanced Diligence, if the third party is assigned a final internal risk rating of 'Low' or 'Medium' it shall be presented to the Chief Compliance Officer for approval to enter into a contractual arrangement with the third party service provider. Notwithstanding any such approval being granted, the Company shall be obligated to comply with its Delegation of Authority Policy before entering into a contractual relationship with the third party.

In general, barring an omission or manifest error during the initial internal risk assessment, a third party which is assigned an initial internal risk rating of 'High' would be highly unlikely to be assigned a final internal risk rating of 'Low' following Enhanced Diligence.

The Company will only transact with a third party which is assigned a final internal risk rating of 'High' if approved by the Compliance Committee which, having reviewed the third party contract in conjunction with the Risk Assessment Procedures Document (as amended from time to time) has concluded that the risk of the third party committing acts of bribery in connection with their engagement with the Company is limited and this risk has been appropriately mitigated through contractual warranties or otherwise. Notwithstanding any such approval being granted, the Company shall be obligated to comply with its delegation of authority policy before entering into a contractual relationship with the third party.

Any third party not approved under Section 4.3 or Section 4.4 shall be barred from reapplying for the same or a substantially similar role for a minimum period of six (6) months (unless the Chief Compliance Officer determines otherwise) and shall, regardless of the role which the third party applies for, be subject to Enhanced Diligence.

If a member of Savannah Staff believes that a third party is engaging in corrupt activity, he or she must immediately notify the Chief Compliance Officer or the Chief Executive Officer. It is the responsibility of the Chief Compliance Officer to examine the activity and to determine the appropriate course of action, including, in consultation with legal counsel, the reporting of corrupt activity to government authorities in accordance with Applicable Laws and regulations.

4.5 Contract Terms

All third parties must be engaged by the Company through a formal written contract. The contract must, at a minimum, address the following elements:

a) compensation structure;
b) any discounts;
c) the types of services being performed;
d) whether fees are tied to results (such as the Company entering into a contract) in the form of commissions or paid on a flat-fee basis;
e) anti-corruption provisions appropriate to the bribery risk which the third party presents to the Company; and
f) the provision by the third party of anti-corruption certificates at the Company's request.

4.6 Monitoring

The Company shall monitor the third party's activities after engagement.

The Chief Compliance Officer shall conduct an annual review in order to ascertain whether the Company's assessment of the bribery risk which each third party presents to the Company remains valid.

Reviews and audits may also be conducted as necessary in the discretion of the Company. When conducting such reviews and audits the Company may take into account any matters which it deems appropriate, including but not limited to the issues highlighted in this Section.

4.7 Acquisitions of Businesses or Teams

When considering the acquisition of businesses, particularly those involving the acquisition of new employees, the Company shall undertake a due diligence process approved by the Compliance Committee.

4.8 Risk Assessment and Anti-Corruption Due Diligence

The main reasons behind the requirement for due diligence are as follows:

a) to try to establish that third parties in any way acting on the Company's behalf are suitable for this purpose. The intention is to minimise any risk that a third party shall take any actions that could breach any anti-corruption laws for which ultimately the Company and Savannah Staff could be held responsible.

b) to try to ensure that the individuals and entities that the Company does business with are engaged in legitimate businesses. The purpose here is to minimise any risk that the Company engages with any person or entity engaged in money laundering or other illicit activities (see Section 6.1 regarding anti-money laundering due diligence); and

c) to try to ensure that the Company does not have dealings with a third party that would result in the Company or Savannah Staff falling into disrepute.

4.9 Local Legal Framework

The laws of the jurisdiction in which the third party shall operate could affect the means by which the Company may engage, utilise and terminate its contractual arrangements with the third party. The Company shall take appropriate legal advice in such circumstances.

5. ANTI-MONEY LAUNDERING POLICY

5.1 Background

The Company's goal is to conduct its operations in a manner that allows Savannah Staff, facilities, products and services to be used only for legitimate business purposes. The Company has adopted this Policy to educate Savannah Staff about money laundering and to establish guiding principles and consistent global standards designed to protect the Company from being used to facilitate money laundering or other illicit activities.

Effective prevention begins with Savannah Staff. Therefore, all Savannah Staff must familiarise themselves with this Policy and understand how to prevent, detect, and refer suspicious activities and transactions to the Group Chief Compliance Officer for review and assessment.

5.2 What is Money Laundering?

Money laundering is broadly defined as the attempt to conceal the origin and ownership of the proceeds of illegal activity and to disguise assets to make them appear legitimate. Broadly, there are considered to be three stages to money laundering, which may comprise of numerous transactions by the launderers that could alert an institution to a criminal activity:

a) **placement** – the stage where cash first enters the financial system and is converted into monetary instruments, such as money orders or travellers cheques, or deposited into accounts at financial institutions;

b) **layering** – the stage where funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin; and

c) **integration** – the stage where funds are reintroduced into the economy in such a way that the source of the funds appears legitimate.

Money laundering can involve the proceeds of any serious crime including, but not limited to, drug trafficking, insider trading, bribery, tax evasion, embezzlement, and securities, bank, wire or mail fraud. Money may also be laundered to conceal its original source in order to finance criminal activities, such as terrorism, or to conceal its original owner, such as persons that are listed on the U.S. Office of Foreign Assets Control's lists of prohibited persons and countries.

Money laundering transactions need not involve cash and can involve any type of financial transaction, including cheque deposits, withdrawals, transfers or movements of funds, securities or other property.

Moreover, money laundering can consist of either a single transaction or a pattern of transactions or complex activities.

In most countries, it is a crime to conduct or to assist in a financial transaction with 'knowledge' or 'wilful blindness' that the transaction involves the proceeds of criminal activity. 'Wilful blindness,' or the deliberate failure to ask questions when the suspicions of a member of Savannah Staff are aroused, may result in the person being charged with the crime of money laundering to the same degree as if the person had been told explicitly that the funds were derived from criminal activity.

It is also illegal to receive funds with 'knowledge' that they are criminally derived.

In the UK, it is a crime under POCA for a person:

a) to conceal, disguise, convert, transfer criminal property or remove criminal property from England and Wales or from Scotland or from Northern Ireland;
b) to enter into or become concerned with an arrangement which he or she knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person;
c) to acquire, use or possess criminal property; and/ or
d) who knows or suspects that a money laundering investigation is being conducted or is about to be conducted to make a disclosure which is likely to prejudice the investigation or to falsify, conceal or destroy documents relevant to the investigation, or cause that to happen.

For the purposes of this Section 5.2, property is criminal property if the alleged offender knows or suspects that the property constitutes or represents benefit from a criminal conduct.

6. ANTI-MONEY LAUNDERING PROCEDURES

6.1 Anti-Money Laundering Due Diligence

The Company's goal is to only do business with counterparties engaged in legitimate business activities and who derive their income, wealth, funds and investable assets from legitimate sources. By dealing only with such counterparties who are known to the Company through the implementation of proper due diligence efforts, the Company can minimise the risk of transacting business with or entering into joint ventures with, or on behalf of, a person engaged in money laundering or other illicit activities.

Consistent with this important objective, before establishing a business relationship with a counterparty or entering into any other business relationship on behalf of the Company, the Company and Savannah Staff must have:

a) complied with all applicable Company procedures for establishing counterparty business relationships; and

b) performed sufficient due diligence to be confident in the legitimacy of the proposed transaction, including the lawfulness of the transaction and the source of funds.

The Company has tailored its counterparty due diligence procedures to address the potential money laundering risks that may be associated with particular types of counterparties, jurisdictions, business lines or methods of doing business.

The anti-money laundering due diligence process which must be followed by the Company prior to entering into a contractual relationship with a third party is set out in the Company's Risk Assessment Procedures Document (as amended from time to time) and is summarised below.

There is no requirement to conduct anti-money laundering due diligence where:

a) the total contract value is less than $5000;

b) the counterparty is not dealing with public officials on behalf of the Company; and

c) the counterparty a corporate entity that is not a personal service company.

However, if there are any concerns in relation to an arrangement which falls within this exemption from the requirement to conduct anti-corruption due diligence from a money laundering perspective, then they should be raised with the Chief Compliance Officer as soon as possible.

Counterparties which have been categorised by the Company as presenting higher degrees of risk from a corruption perspective shall be required to provide more information and documentation in the context of the Company's anti-money laundering due diligence than those which have been categorised as presenting lower degrees of risk.

Before establishing a business relationship with a counterparty, effecting a transaction or entering into a business transaction on behalf of the Company with a counterparty deemed to be at high risk, the Company requires higher levels of due diligence be performed and Savannah Staff must check with the Group Chief Compliance Officer regarding any additional due diligence procedures that may be required.

The following factors may indicate that a third party should be considered as presenting a high risk from a money laundering perspective:

a) individuals that are either current or former senior foreign or domestic political figures or are friends or relatives of current or former senior foreign or domestic political figures;

b) individuals or entities that are domiciled in a jurisdiction that do not have effective anti-money laundering regimes or where there is a high incidence of corruption; or

c) individuals or entities that have been included on a governmental or international organisation's list of terrorists.

6.2 Detecting and Referring Suspicious Activity

Savannah Staff must be alert for possible money laundering or suspicious activity. Any participation by Savannah Staff in money laundering, either with knowledge or through wilful blindness, is strictly prohibited. Savannah Staff must not advise or assist anyone who is attempting to avoid money laundering laws or circumvent this Policy and its implementing procedures.

Under no circumstances may any member of Savannah Staff inform or 'tip off' any party involved in suspicious or illegal activity that his, her or its activities are believed to be suspicious, are being referred within the Company or reported to government authorities, or are being investigated by the authorities.

If a member of Savannah Staff believes that a transaction is suspicious, he or she must immediately notify the Chief Compliance Officer or the Chief Executive Officer. It is the responsibility of the Chief Compliance Officer to examine the activity and to determine whether the activity is suspicious, with the goal that appropriate action is taken, including, in consultation with legal counsel, the reporting of suspicious activity to government authorities in accordance with Applicable Laws and regulations.

Cash and Cash Equivalents

In order to reduce the risk of the Company's inadvertent involvement in money laundering schemes, the Company requires documentation of the handling of cash and cash equivalents (for example,

cheques, money orders, etc.). This documentation is designed to prevent money launderers from using the Company to evade cash and cash equivalent reporting requirements.

The Chief Compliance Officer shall review this documentation for suspicious activity that may implicate cash reporting requirements.

7. SCHEDULE I OFFENCES UNDER THE BRIBERY ACTS

7.1 Penalty and Jurisdiction

Offences under the Bribery Act are punishable for individuals by up to ten (10) years' imprisonment and a fine. If the Company is found to have taken part in corruption, it could face an unlimited fine, be excluded from tendering for public contracts and face damage to its reputation. The Company therefore takes its legal responsibilities very seriously.

The English courts shall have jurisdiction over general bribery offences and bribery of foreign government official offences (as described below) which are committed in the UK. They shall also have jurisdiction over such offences if they are committed outside the UK if the person committing them has a close connection with the UK by virtue of being a British national or ordinarily resident in the UK, a body incorporated in the UK or a Scottish partnership.

8. GENERAL OFFENCES

The Bribery Act sets out two general offences which broadly relate to (i) offering bribes and (ii) accepting bribes. The general offences are aimed at the situation where, either in business or in performing a public role, someone who is supposed to be acting in good faith or impartially, or who is in a position of trust, is offered or takes a bribe.

The general offences apply in relation to the Company's dealings with all persons, including UK and non-UK public officials.

One of the consequences of the general offences is that facilitation payments, which are payments made outside of the ordinary course of business in order to facilitate or speed up performance of bureaucratic processes, are illegal. Facilitation payments are therefore prohibited by the Company.

9. FAILURE OF A COMMERCIAL ORGANISATION TO PREVENT BRIBERY

Under the Bribery Act a commercial organisation is guilty of an offence if a person associated with it bribes another person intending to obtain or retain business or a business advantage for the commercial organisation. It is irrelevant for these purposes whether that person is a UK national or resident in the UK, or a body incorporated or formed in the UK.

It also does not matter whether the acts or omissions which form part of the bribery offence take part in the UK or elsewhere.

The definition of a person who 'performs services for or on behalf of' the organisation is intended to give the offence broad scope so as to encompass all persons connected to an organisation who might be capable of committing bribery on the organisation's behalf.

This broad scope means that contractors could be 'associated' persons to the extent that they are performing services for or on behalf of a commercial organisation. Moreover, where a supplier can properly be said to be performing services for a commercial organisation rather than simply acting as the seller of goods, it may also be an 'associated' person.

It is a defence for a commercial organisation to prove that despite a particular case of bribery taking place, it nevertheless had in place adequate procedures designed to prevent its associated persons from bribing.

In March 2011, The Ministry of Justice published guidance about procedures that commercial organisations can put in place to prevent persons associated with them from bribing on their behalf (the "**Guidance**"). The Guidance does not have the force of law and can be revised by the Secretary of State at any time.

The Guidance states that the question of adequacy of bribery prevention procedures shall depend in the final analysis on the facts of each case, including matters such as the level of control over the activities of the associated person and the degree of risk that requires mitigation.

10.PAYMENTS TO FOREIGN PUBLIC OFFICIALS

The Bribery Act creates a standalone offence for the bribery of a foreign public official.

A 'foreign public official' includes officials, whether elected or appointed, who hold a legislative, administrative or judicial position of any kind of a country or territory outside the UK.

It also includes any person who performs public functions in any branch of the national, local or municipal government of such a country or territory or who exercises a public function for any public agency or public enterprise of such a country or territory, such as professionals working for public health agencies and officers exercising public functions in state-owned enterprises.

Foreign public officials can also be an official or agent of a public international organisation.

The offence is committed where a person offers, promises or gives a financial or other advantage to a foreign public official with the intention of influencing the official in the performance of his or her official functions. The person offering, promising or giving the advantage must also intend to obtain or retain business or an advantage in the conduct of business by doing so.

The offence is not committed where the official is permitted or required by the applicable written law to be influenced by the advantage.

SCHEDULE 1 CERTIFICATE COMPLIANCE

The undersigned hereby certifies that he, she or they has or have read, understands and agrees to comply with the Company's Anti-Corruption and Money Laundering Policy.

Signature: _____

Name: _____

Date: _____

The above signed also certifies that the following employees have undertaken the same:

Name(s) of participant(s): _____

_____

_____

SCHEDULE 2 CERTIFICATE OF TRAINING

The undersigned hereby certifies that he, she or they has or have received anti-bribery and corruption training.

Signature: _____

Name: _____

Date: _____

Name of training: _____

Date of training: _____

The above signed also certifies that the following employees have undertaken the same:

Name(s) of participant(s): _____

_____

_____