ANTI-MONEY LAUNDERING AND SANCTIONS COMPLIANCE POLICY

SEACREST PETROLEO BERMUDA LIMITED

1. PURPOSE

Seacrest Petroleo Bermuda Limited ("**Seacrest Petroleo**") and its subsidiaries and affiliates (collectively, the "**Group**" and each, individually, a "**Group Company**") are committed to full compliance with all applicable laws and regulations regarding anti-money laundering and Sanctions compliance. Each Group Company will comply with and enforce the provisions set forth in this Anti-Money Laundering and Sanctions Compliance Policy (this "**AML and Sanctions Compliance Policy**") in order to detect and prevent money laundering and terrorist financing and avoid any breaches of applicable Sanctions. As used herein, "**Sanctions**" means any sanctions, regulations, embargoes or other restrictive measures that have been enacted, imposed or enforced by Norway, the United Kingdom, the United States of America, Bermuda or Brazil, or by their respective government agencies or administrative bodies, or by the United Nations, the European Union, the World Bank or other international organizations.

If any Group Company, its personnel and/or premises are inadvertently used for money laundering or other illegal activities or if any Group Company violates applicable Sanctions, the Group can be subject to potentially serious civil and/or criminal penalties. Therefore, it is imperative that every director, officer, employee, representative or contractor of any Group Company ("**Group personnel**") is familiar with and complies with the policies and procedures set forth in this AML and Sanctions Compliance Policy. This AML and Sanctions Compliance Policy is to be strictly adhered to by all Group Personnel. Non-compliance by any Group personnel shall result in disciplinary action. There are no exceptions to this AML and Sanctions Compliance Policy without the prior written approval of the Group's Chief Compliance Officer (the "**CCO**"). Any questions, comments or concerns regarding this AML and Sanctions Compliance Policy should be directed to the CCO.

2. SCOPE AND APPLICATION

This AML and Sanctions Compliance Policy applies to all Group Companies and all Group personnel. The Group's activities involve commercial counterparties in the oil and gas exploration and production industry and related service industries (collectively, "**Counterparties**" and each, individually, a "**Counterparty**"). The Group will only engage in activities with Counterparties that will be fully compliant with all applicable anti-money-laundering and terrorist financing rules and regulations and which are not subject to applicable Sanctions.

3. COMPLIANCE

The CCO is responsible for ensuring that Group Companies and Group personnel comply with this AML and Sanctions Compliance Policy. Group personnel shall immediately notify the CCO if he/she (i) is informed that a Counterparty is suspected of engaging in illegal activity, or (ii) suspects or has any reason to suspect that any potentially suspicious activity has occurred or will occur with respect to a transaction that he/she is engaged in. Group personnel are encouraged to seek the assistance of the CCO with any questions or concerns they may have with respect to this AML and Sanctions Compliance Policy.

The CCO shall:

- coordinate and monitor the Group's day-to-day compliance with applicable anti-

money laundering laws and regulations and applicable Sanctions;
- receive and review any reports of suspicious activity from Group personnel or a Counterparty;
- determine whether any suspicious activity reported by Group personnel or a Counterparty warrants reporting to Management and/or filing a Suspicious Activity Report (an "**SAR**") with the appropriate authorities;
- coordinate due diligence procedures regarding Counterparties; and
- respond to both internal and external inquiries regarding this AML and Sanctions Compliance Policy.

4. SANCTIONS

Applicable Sanctions generally prohibit or restrict all or certain types of transactions involving specified countries (the "**Embargoed Countries**") or transactions or other dealings with named individuals and entities, or entities controlled by them ("**Denied Parties**"), located in Embargoed Countries, as well as others. Denied Parties can be "front" companies or other entities owned or controlled by targeted countries or groups, specially identified individuals such as terrorists or narcotics traffickers, or groups affiliated with an individual. Prohibited transactions broadly include both direct dealings with Embargoed Countries and Denied Parties and indirect dealings that facilitate prohibited transactions. The databases listing Embargoed Countries and Denied Parties are constantly updated by the relevant national and supranational authorities, which means that Group personnel responsible for compliance with this AML and Sanctions Compliance Policy must regularly check those databases. Sanctions that generally prohibit any dealings with any individual or entity in an Embargoed Country, regardless of the involvement of a Denied Party, are referred to herein as "**Blocking Sanctions**".

No Group Company shall enter into any transaction with a prospective Counterparty who is a Denied Party or who is in an Embargoed Country, nor shall any Group Company have any dealings with any individual or entity who is subject to Blocking Sanctions. The databases listing Embargoed Countries and Denied Parties can be searched online at:

- https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions
- https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets
- https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx
- https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases
- https://eeas.europa.eu/topics/sanctions-policy/8442/consolidated-list-of-sanctions_en
- https://sanctionssearch.ofac.treas.gov/
- https://www.export.gov/csl-search
- https://scsanctions.un.org/search/

No Group Company shall ask a third party to undertake or arrange a transaction with an individual or entity that it could not make itself. If a third party asks for help in arranging a transaction with a Denied Party or an individual or entity in an Embargoed Country or that is subject to Blocking Sanctions, that request should be turned down and the CCO immediately informed of the request.

If any Group personnel suspect that someone is attempting to circumvent this AML and Sanctions Compliance Policy by disguising their identity or providing incomplete information, the relevant lists of Denied Parties should be reviewed to determine whether any participants in, or beneficiaries of,

the potential transaction are designated as Denied Parties. The relevant lists are accessible at the URLs identified above.

Any Group Personnel with questions concerning Sanctions compliance, including but not limited to questions related to a past matter, a current matter, or a new Counterparty, should contact the CCO.

Failure to comply with this AML and Sanctions Compliance Policy may be grounds for termination or other disciplinary action.

5. COUNTERPARTY IDENTIFICATION PROCEDURES

General

Prior to accepting funds from, or entering into a transaction with, a prospective Counterparty, all reasonable and practical measures must be taken to confirm the Counterparty's identity and ensure that a Prohibited Counterparty (as defined below) is not accepted ("**Counterparty Identification Procedures**"). Group personnel should review and be familiar with the following so as to be in a position to detect suspicious or illegal activity.

These Counterparty Identification Procedures are based on the premise that funds will be accepted from, and transactions entered into with, a new or existing Counterparty only after:

- the Counterparty's identity has been confirmed and that the Counterparty is acting as a principal and not for the benefit of any third party unless specific disclosure to that effect is made; or

- if the Counterparty is acting on behalf of others, the identities of the underlying third parties has been confirmed.

Counterparty Identification Procedures for Natural Persons

In order to confirm the identity of a Counterparty, copies of certain of the following documents will be obtained and retained for the Group's records as appropriate under the circumstances:

- Driver's license, passport or other official government-issued identification of main individuals representing a Counterparty; and
- EIN or social security number (U.S. taxpayers only).
- Additional information which may be requested includes:
- Bank statement or utility bill; or other residential identifying information;
- Credit report; and/or
- Personal/bank references.

Counterparty Identification Procedures for Corporations, Partnerships, Trusts and Other Legal Entities

If the Counterparty is not a publicly-traded company listed on an organized exchange (or a subsidiary or a pension fund of such a company) or a regulated institution organized in a Financial Action Task Force on Money Laundering Compliant Jurisdiction (see http://www.fatf-gafi.org/countries/#FATF), the Group should obtain certain of the following, as appropriate under the circumstances:

- Evidence that the Counterparty has been duly organized in its jurisdiction of

organization;
- Information on Counterparty's ownership structure and ultimate beneficial owners, with supporting documents, if appropriate;
- Authorized signatory list;
- EIN (U.S. taxpayers only);
- Certification from the Counterparty that it has implemented and complies with applicable anti-money laundering policies, procedures and controls ("AML Certificate") (if the Compliance Officer believes it is reasonable to rely upon a certification from the Counterparty);
- In the case of a trust, evidence of the trustee's authority to make the contemplated investment and either an AML Certificate from the trustee (if the Compliance Officer believes it would be reasonable to rely upon such a certificate) or, alternatively, the identities of beneficiaries, settlor(s), trustee(s) and any persons who have the power to remove trustees, as well as of authorized activity of the trust and the persons authorized to act on behalf of the trust;
- Publicly available information from law enforcement agencies or regulatory authorities; and/or
- Counterparty's annual report.

High-Risk Counterparties

Seacrest Petroleo Personnel shall endeavor to determine whether any potential Counterparty of a Group Company is a "High Risk Counterparty". In the event that a potential Counterparty may be considered to be a "High Risk Counterparty", Seacrest Petroleo Personnel shall inform the Compliance Officer prior to the conduct of any business with such potential Counterparty. The Compliance Officer, in his sole discretion, shall determine which, if any, of the enhanced identification procedures are necessary to confirm the identity and the source of the funds of the potential Counterparty and Seacrest Petroleo Personnel shall not conduct business with the High Risk Counterparty until granted permission by the Compliance Officer.

The following types of Counterparties are considered to pose a high money laundering risk (see Exhibit A for definitions) and as such are considered "High Risk Counterparties":

- A Senior Foreign Political Figure, any member of a Senior Foreign Political Figure's Immediate Family, and any Close Associate of a Senior Foreign Political Figure;
- Any Counterparty resident in, or organized or chartered under the laws of, a Non-Cooperative Jurisdiction;
- Any Counterparty who gives the Compliance Officer any reason to believe that its funds originate from, or are routed through, an account maintained at a bank organized or chartered under the laws of a Non-Cooperative Jurisdiction; and
- Any Counterparty who gives the CCO any reason to believe that the source of its funds may not be legitimate or may aid terrorist activities.

Enhanced Counterparty Identification Procedures for 'High-Risk' Natural Persons

Enhanced Counterparty Identification Procedures for 'high risk' natural persons as Counterparties include, but are not limited to, the following:

- Reviewing pronouncements of multilateral organizations such as the FATF with regard to the adequacy of anti-money laundering and counter-terrorism legislation in the Counterparty's home jurisdiction;
- Assessing the Counterparty's business reputation through review of financial or professional references, generally available media reports or by other means;

- Considering the source of the Counterparty's wealth, including the economic activities that generated the Counterparty's wealth, and the source of the particular funds intended to be used to make the investment;
- Reviewing generally available public information, such as media reports, to determine whether the Counterparty has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any investigation, indictment, conviction or civil enforcement action relating to financing of terrorists;
- Reviewing the Counterparty's last tax return, financial statements and/or bank statements; and
- Conducting a face-to-face meeting with the Counterparty to discuss/confirm the account opening documents, purpose of account and source of assets.

Enhanced Counterparty Identification Procedures for 'High-Risk' Corporations, Partnerships, Trusts and Other Legal Entities

Enhanced Counterparty Identification Procedures for 'high risk' corporations, partnerships and other legal entities include, but are not limited to, the following:

- Reviewing pronouncements of multilateral organizations such as FATF with regard to the adequacy of anti-money laundering and counter-terrorism legislation in the Counterparty's home country jurisdiction;
- Assessing the Counterparty's business reputation through review of financial or professional references, generally available media reports or by other means;
- Reviewing recent changes in the ownership or senior management of the Counterparty;
- Conducting a visit to the Counterparty's place of business and conducting a face-to-face meeting with the Counterparty to discuss/confirm the account application, the purpose of the account and the source of assets;
- Reviewing annual reports for the past year and financial statements for the past three years (if available);
- If applicable, determining the relationship between the Counterparty and the government of its home country jurisdiction, including whether the Counterparty is a government-owned entity; and
- Reviewing generally available public information to determine whether the Counterparty has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any criminal investigation, indictment, conviction or civil enforcement action relating to financing of terrorists.

Prohibited Counterparties

The Compliance Officer shall also maintain a current list of prohibited Counterparties from or on behalf of whom funds will not be accepted or to whom funds will not be disbursed ("**Prohibited Counterparties**"). Prohibited Counterparties include:

- Any Counterparty who is a Denied Person (including, without limitation, whose name appears on the List of Specially Designated Nationals and Blocked Persons maintained by the U.S. Office of Foreign Assets Control ("**OFAC**"), which may be found at https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx) or the List of Designated Persons: Terrorism and Terrorist Financing, which may be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664

723/Terrorism_and_Terrorist.pdf) or who is in an Embargoed Country;
- Any Counterparty who is subject to Blocking Sanctions;
- High-risk Counterparties that have not satisfied the enhanced due diligence requirements, as set forth above; and
- Those who are named on such other lists of prohibited persons and entities as may be mandated by applicable law or regulation.

Counterparty Records Retention

With respect to each Counterparty, the CCO shall retain copies of all documents related to the Counterparty Identification Procedures for an appropriate period of time and, at a minimum, the period of time required by applicable law or regulation.

Review of Existing Counterparty Base and Detection of Suspicious Activity

The CCO shall coordinate a periodic review of the Group's existing Counterparty list in order to verify that no Counterparty is a Prohibited Counterparty, and to ensure the adequacy of due diligence performed on existing Counterparties. In addition, in some circumstances, the following activities, none of which per se constitutes suspicious activity, may be indicative of Counterparty activity that may require further investigation:

- Counterparty exhibits an unusual concern regarding the compliance with government reporting requirements, particularly with respect to the Counterparty's identity, type of business and assets, or Counterparty is reluctant or refuses to reveal any information concerning business activities, or Counterparty furnishes unusual or suspect identification or business documents;

- Counterparty wishes to engage in businesses or investments that are inconsistent with the Counterparty's apparent business/investment strategy;

- Counterparty (or a person publicly associated with the Counterparty) is the subject of news reports indicating possible criminal, civil or regulatory violations;

- Counterparty appears to be acting as the agent for another entity but declines, or is reluctant, without legitimate commercial reasons, to provide any information in response to questions about such entity;

- Counterparty has difficulty describing the nature of his or her business or lacks general knowledge of the industry he or she is apparently engaged in; and

- Counterparty attempts to make or requests transactions in cash or cash equivalents.

Any Group personnel who detect suspicious activity or have reason to believe that suspicious activity is taking place shall immediately inform the CCO. The CCO shall determine whether to report to appropriate law enforcement officials any suspicious activity of which he or she becomes aware.

6. ACCEPTABLE METHODS OF FUND TRANSFERS

The Group will only accept Counterparty funds in the form of:

- A wire transfer through a financial institution incorporated in or with its principal place of business in an FATF country (see http://www.fatf-

gafi.org/countries/#FATF); or

- A bank draft (check) drawn on a financial institution incorporated in or with its principal place of business in an FATF country (other than a third-party check).

7. SUSPICIOUS TRANSACTIONS / FILING A SAR

The Group shall be responsible to file SARs for any account activity (including deposits and transfers) conducted or attempted through a Group Company involving $5,000 or more where the Group knows, suspects, or has reason to suspect that: (a) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation, (b) the transaction has no business or apparent lawful purpose or is not the sort in which the Counterparty would normally be expected to engage, and the Group knows, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or (c) the transaction involves the use of a Group Company to facilitate criminal activity.

The Group shall not base the decision on whether to file an SAR solely on whether the transaction falls above a set threshold. The Group will file an SAR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. In high-risk situations, the Group will notify the government immediately and will file an SAR with the relevant state authority.

8. TRAINING PROGRAM

As part of the Group's AML and Sanctions Compliance program, all Group Personnel are expected to be fully aware of, and to read and comply with, this AML and Sanctions Compliance Policy. All Group personnel are required to address any questions and concerns to the CCO. To ensure continued adherence to this AML and Sanctions Compliance Policy, all Group personnel will be required to attend training classes at which this Policy and any new developments in money laundering and Sanctions compliance will be addressed.

ADOPTED: October 20, 2020

Exhibit A

DEFINITIONS

A "**Close Associate of a Senior Foreign Political Figure**" is a person who is widely and publicly known internationally to maintain an unusually close relationship with the Senior Foreign Political Figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the Senior Foreign Political Figure.

An "**FATF-Compliant Jurisdiction**" is a jurisdiction that (i) is a member in good standing of FATF and (ii) has undergone two rounds of FATF mutual evaluations.

"**FATF**" means the Financial Task Force on Money Laundering.

The "**Immediate Family of a Senior Foreign Political Figure**" typically includes the political figure's parents, siblings, spouse, children and in-laws.

"**Non-Cooperative Jurisdiction**" means any foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization, such as the FATF.

"**Senior Foreign Political Figure**" means a senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned corporation. In addition, a Senior Foreign Political Figure includes any corporation, business or other entity that has been formed by, or for the benefit of, a Senior Foreign Political Figure.