# COBRA RESOURCES PLC

## AML AND COUNTER-TERRORIST FINANCING POLICY

## 1. INTRODUCTION AND SCOPE OF THIS POLICY

1.1 This policy (the "**Policy**") sets out an overview of the anti-money laundering ("**AML**") and counter-terrorist financing ("**CTF**") regime in the United Kingdom and the steps Cobra Resources plc (the "**Company**" or "**we**" and as the context requires, shall include any group companies) have taken and procedures we have put in place to comply with our statutory and regulatory obligations in relation to the prevention of money laundering and terrorist financing.

1.2 We are committed to preventing the carrying out of operations that may be related to money laundering or the funding of terrorism by establishing policies on internal control, risk assessment, risk management and compliance. We shall comply with our obligations in law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering or funding of terrorism through the abuse of our systems and/or services.

## 2. DEFINITIONS

2.1 The primary laws and regulations behind the UK's AML and CTF regime are to be found in:

(a) Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the "**Regulations**");

(b) the Proceeds of Crime Act 2002 ("**POCA**");

(c) Terrorism Act 2000 ("**TA 2000**");

(d) HM Treasury Sanctions Notices and Guidance and News Releases ("**Financial Sanctions**"); and

(e) Financial Crime Guide: A firm's guide to countering financial crime risks (the "**Guidance**" or **"FCG**").

2.2 Another source of guidance is the Joint Money Laundering Steering Group Guidance ("**JMLSG**") available at www.jmlsg.org.uk/industry-guidance/article/guidance.

2.3 The following definitions are set out for the purposes of this Policy:

(a) **Money Laundering**

The term "money laundering" describes the process of the conversion of the proceeds of crime into legitimate currency or other assets.

Typically, there are three stages to the money-laundering process:

(i) **Placement** – describes the initial introduction of the proceeds of crime into the legitimate financial system;

(ii) **Layering** – is the passing of proceeds through a series of transactions so as to obscure their origin; and

(iii) **Integration** – is the reappearance of the laundered proceeds as apparently legitimate funds or assets.

Money laundering may take many forms including, attempts to convert money raised through criminal activity into legitimate or "clean" money, handling the benefit of acquisitive crimes (such as fraud and tax evasion), entering into arrangements which facilitate the laundering of criminal property, and criminals investing the proceeds of their crime in commercial, financial or real estate transactions.

Money laundering and terrorist financing are closely related to the risks of other financial crime such as fraud and tax evasion. Although fraud and tax evasion are not dealt with in this Policy, this Policy does apply to the proceeds of crime that arise from those activities.

(b) **Terrorist Financing**

Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organisations.

There can be considerable similarities between the movement of terrorist property and the laundering of criminal property. However, one of the primary differences between terrorist property and criminal property more generally, is that terrorists can be funded from legitimately obtained income, which can make it difficult to identify the stage at which legitimate funds become terrorist property.

(c) **Financial Sanctions**

Financial Sanctions are restrictions put in place by the UN, EU, UK or US to achieve a specific foreign policy or national security objective. They can limit the provision of certain financial services and restrict access to financial markets, funds and economic resources.

Financial Sanctions come in many forms as they are developed in response to a given situation. The most common types of Financial Sanctions used in recent years are:

(i) **Targeted asset freezes** – these apply to named individuals, entities and bodies, restricting access to funds and economic resources; and

(ii) **Restrictions on a wide variety of financial markets and services** – these can apply to named individuals, entities and bodies, specified groups, or entire sectors and can take the form of investment bans, requirements to notify or seek authorisation prior to certain payments being made or received, and restrictions on the provision of financial or advisory services or other financial assistance.

2.4 Unless the context otherwise requires words and expressions used in these Policies shall have the same meaning as that set out in the Regulations.

## 3. RISK MANAGEMENT

3.1 We take a risk-based approach to monitoring the financial activities of customers. We have undertaken a risk assessment to identify and assess the risks of money laundering and terrorist financing, including assessment of our customers, geographic areas of operation, products and service, transactions and delivery channels.

3.2 Fitting with our risk assessment, the Company shall not conduct or knowingly allow illegal or unacceptable-risk related economic activity of individual Client or Intermediary, including, but not limited to: gambling, adult related content, firearms or other weapons, escort services, copyright violations, human trafficking, sanction or embargo avoidance related activity or any other activity which may be illegal in the country where it's conducted.

3.3 Clients or Intermediaries engaged in any of the above activities will be beyond the Company's risk appetite and considered as prohibited Clients. The Company will not enter into business relationship or partnership with such Clients, and, if the above-mentioned circumstances are discovered once the business relationship is already established or the existing Client engages in new activity from the above list, the Company will consider limiting or terminating such business relationship. The decision to continue such business relationship can only be made by the Chief Executive Officer of the Company (the "**CEO**").

3.4 Risk appetite shall be regularly reviewed based on the outcomes of internal Company-wide risk assessment carried out annually and/or when expanding subsidiaries to new geographical markets. The risk assessment shall also be performed for each new product or service offered by the Company prior to its provision to the Clients as well as when the Company suspects or becomes aware of any change in circumstances that may affect the level of risk attributed to particular product or service.

3.5 The risk assessment shall also be performed prior to commencement of the Company's activities, as well as during business prior to extending the investment directions. Also, risk assessment, full or limited scope, shall be carried out before targeting new Client segment, introducing new delivery channel, etc..

3.6 Risk assessment shall capture changes in inherent and residual risks, if any, related to Client base, products, delivery channels, and geographies the Company is operating in. The format of risk assessment will be approved by the board of directors of the Company (the "**Board**"). The CEO or money laundering reporting officer (the "**MLRO**") will be responsible for organizing the risk assessment activity or delegating this task to another competent employee. The information needed to properly carry out a risk assessment will be provided by employees of the Risk Management and Compliance Unit, as well as business responsible. The outcomes of every risk assessment in a documented form shall be presented to and approved by the Board.

## 4. INTERNAL CONTROLS

4.1 Greg Hancock is responsible for Anti-Money Laundering Compliance for the Company and will be the nominated officer for suspicious activity reporting ("**MLRO**").

4.2 We will ensure that when new technology is adopted, appropriate measures are taken to assess and, if necessary, mitigate any money laundering or terrorist financing risks this technology may cause.

4.3 The MLRO shall periodically (at least once a year) or upon occurrence of important events or changes (for instance, on changes in legal acts or when new risks relevant to the Company arise) revise this Policy and update it, if needed.

4.4 The Company shall perform a periodic audit of anti-money laundering and terrorist financing prevention measures applied in the Company. The CEO shall be responsible for the organisation of the periodic audit. Such periodic reviews and audits shall be performed by an internal auditor or an independent third party. The testing results shall be recorded in a written form. The final report shall be presented to the Board.

4.5 The audit shall be risk-based and evaluate the quality of risk management for all operations, departments.

4.6 The testing results shall be recorded in a written form. The final report, along with a detailed plan to remedy the identified deficiencies, shall be presented to the Board.

## 5. SUSPICIOUS ACTIVITY REPORTING

5.1 If an employee has grounds for knowledge or suspicion of money laundering or terrorist financing, they are obligated to report this to the MLRO as soon as reasonably practicable using the form in Annex 1 of this Policy. The MLRO will maintain a log of suspicious activity reports, in the form provided in Annex 2.

5.2 The MLRO will then determine whether a Suspicious Activity Report ("**SAR**") will be made to the National Crime Agency ("**NCA**"). Any further transactions or business with that customer should be reported to the nominated officer until such time as the nominated officer determines that no report should be made.

5.3 Further details on the NCA and SARs can be found at http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars.

5.4 It is a criminal offence for anyone, following a disclosure to a MLRO or to the appropriate agency, to do or say anything that might either 'tip off' another person that a disclosure has been made or otherwise prejudice an investigation.

5.5 We will, as part of our staff training, make certain all staff are aware of the requirement to submit suspicious activity reports where they have grounds for that suspicion and that they must not do or say anything to anyone about that report and its contents.

## 6. CUSTOMER DUE DILIGENCE

6.1 We are committed to knowing its customers appropriately before establishing a business relationship. To verify a customer's identity, we have established customer due diligence ("**CDD**") and Know-Your-Client ("**KYC**") procedures.

6.2 KYC procedures must be followed before the Company establishes a business relationship or carries out an occasional transaction.

6.3 We take a risk-based approach to KYC, and the amount of information that is required may vary depending on risk factors. However, as a minimum, we will need to:

(a) identify the customer;

(b) verify the identity of the customer;

(c) identify and verify the identity of the beneficial owner(s) (where relevant); and

(d) verify the purpose and intended nature of the business relationship or transaction.

6.4 The beneficial owner, in relation to a body corporate (including a UK limited liability partnership but excluding a company listed on a regulated market), means an individual who exercises ultimate control over the management of the body corporate, or ultimately owns or controls (whether directly or indirectly) more than 25% of the shares or voting rights in the body corporate, or otherwise controls the body. In relation to a partnership (other than a limited liability partnership), the beneficial owner means an individual who is entitled to or controls (whether directly or indirectly) more than 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership, or otherwise exercises ultimate control over the management of the partnership.

6.5 Identification of a customer or beneficial owner simply means being told or coming to know a customer's identifying details, such as their name and address. Verification is obtaining some evidence which supports this claim of identity.

6.6 To identify the customer, if the customer is an individual or a small, unincorporated partnership, we require the following information:

(a) full name;

(b) residential address; and

(c) date of birth.

6.7 In order to verify the customer's identity, we will require the following documents:

(a) a government-issued document which incorporates the customer's full name and photograph and either their residential address or their date of birth. For example:

(i) valid passport;

(ii) valid photocard driving licence (full or provisional); or

(iii) national Identity card; and

(b) a second document, either government-issued, or issued by a judicial authority, a public-sector body or authority, a regulated utility company. For example:

(i) current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in the UK or EU, or utility bills (issued within the last three months); or

(ii) current council tax demand letter, or statement.

6.8 To identify the customer, if the customer is a private company, limited liability partnership or large partnership we require the following information:

(a) full name;

(b) the company number or other registration number;

(c) the address of the registered office and principal place of business;

(d) the law to which it is subject and its constitution;

(e) the names of the board of directors/partners (or equivalent management body) and senior persons responsible for its operations; and

(f) name of beneficial owner(s).

6.9 In order to verify the identity of a private company, limited liability partnership or large partnership, we may use information obtained through public registers (for example, the UK's Companies House) or may be provided directly by the customer with documents verifying the information, including:

(a) Certificate of Incorporation;

(b) Articles of Association;

(c) Memorandum of Association;

(d) latest Annual Return or Confirmation Statement, with details of current company officers (i.e. directors and company secretary and shareholders); and/or

(e) a capitalisation table.

## 7. SIMPLIFIED DUE DILIGENCE

7.1 There are circumstances where the risk of money laundering and terrorist financing may be low. In these circumstances, provided there has been adequate analysis of the risks, we may apply simplified due diligence ("**SDD**"). The factors that should be taken into account include:

(a) whether the customer:

(i) is a public administration or a publicly owned enterprise;

(ii) is an individual resident in a geographical area of lower risk (see subparagraph (c));

(iii) is a credit institution or a financial institution which is:

(A) subject to the requirements in national legislation implementing the fourth money laundering directive as an obliged entity (within the meaning of that directive); and

(B) supervised for compliance with those requirements in accordance with section 2 of Chapter VI of the fourth money laundering directive;

(iv) is a company whose securities are listed on a regulated market, and the location of the regulated market;

(b) product, service, transaction or delivery-channel risk factors, including whether the product or service is one of the insurance policies, pensions or electronic money products specified in the Regulations; and

(c) geographical risk factors based on where the customer lives or is established and where it does business, for example, an EEA State or third country with effective systems to counter money laundering or terrorist financing or with documented low levels of corruption or other criminal activity.

7.2 Even though we may apply SDD to a customer, we will still need to be satisfied that we are confident of the information in 6.3, although we may adjust the timing or type of measures that we undertake.

## 8. ENHANCED DUE DILIGENCE

8.1 The Regulations prescribe certain circumstances in respect of which enhanced due diligence ("**EDD**") must be applied. These include circumstances where:

(a) the transaction has been identified as one where there is a high risk of money laundering or terrorist financing in our risk assessment or in the information made available to us by our supervisor under the Regulations;

(b) the customer or beneficial owner is a political exposed person ("**PEP**"), or a family member or known close associate of a PEP;

(c) the customer or transaction is in a high risk third country;

(d) wherever the transaction:

(i) is complex and unusually large or there is an unusual pattern of transactions; and

(ii) the transaction or transactions have no apparent economic or legal purpose; or

(e) there is any other situation which can present a higher risk of money laundering or terrorist financing.

8.2 Where such circumstances are identified, we will apply EDD measures which may include:

(a) obtaining additional information on the customer and any beneficial owner;

(b) obtaining additional information on the intended nature of the business relationship, including details concerning the customer's source of wealth and the source of funds;

(c) obtaining the approval of the MLRO to commence the business relationship; and

(d) increasing the degree and nature of monitoring of the business relationship, in order to determine whether the transaction is unusual or suspicious.

## 9. POLITICALLY EXPOSED PERSONS ("PEP")

9.1 The definition of a PEP includes:

(a) heads of state, heads of government, ministers and deputy or assistant ministers;

(b) members of parliament or of similar legislative bodies;

(c) members of the governing bodies of political parties;

(d) members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;

(e) members of courts of auditors or of the boards of central banks;

(f) ambassadors, charges d'affaires and high-ranking officers in the armed forces;

(g) members of the administrative, management or supervisory bodies of State-owned enterprises; and

(h) directors, deputy directors and members of the board or equivalent function of an international organisation.

9.2 Family members of a PEP include a spouse or partner of that person, children of that person and their spouses or partners, and parents of that person.

9.3 Where a customer or beneficial owner is identified as a PEP, the Regulations provide that you must:

(a) obtain the approval of the MLRO to establish or continue the business relationship with the customer;

(b) take adequate measures to establish the source of wealth and the source of funds which are involved in the business relationship or occasional transaction; and

(c) conduct enhanced due diligence.

## 10. ONGOING MONITORING

10.1 Ongoing monitoring will be undertaken in a risk-based manner in accordance with the customer risk assessment. Customers which present a greater risk may be subject to more stringent or frequent monitoring. Ongoing monitoring will include the following:

(a) transaction monitoring for unusual or suspicious transactions;

(b) update to PEP and sanctions lists; and

(c) KYC updates.

10.2 Employees responsible for KYC shall perform and document reviews of each Clients' activities to make sure information submitted by Clients and the Company's knowledge of Clients is consistent.

10.3 Information collected about Clients assigned to the low risk group shall be renewed at least once every 3 years.

10.4 Information collected about Clients assigned to the medium risk group shall be renewed at least once every 2 years.

10.5 Information collected about Clients assigned to the high risk group shall be renewed at least once a year.

10.6 Renewal of information shall cover at least all the information of KYC procedure.

10.7 Verification is repeated or requests for additional information are communicated to a (potential) Client when there are doubts about veracity or adequacy of previously obtained identification data.

## 11. RELIANCE AND RECORD KEEPING

11.1 All due diligence and identity verification will be done by the Company's employees or by one of the Company's partners if the company outsources the identity verification to a third party.

11.2 Due diligence and identity verification will only be outsourced if we have agreements in place that allow for customer due diligence to be conducted by the partner on behalf of the Company, in accordance with the rules and procedures set out in this Policy and applicable law. This does not absolve our obligation to comply with anti-money laundering regulations and it is the responsibility of the Company's employees to review the information sent and ensure it is in keeping with this Policy.

11.3 All records relating to anti-money laundering compliance and due diligence will be retained for at least 5 years. This includes customer information, transactions, SARs, annual anti-money laundering reports and training and compliance monitoring.

11.4 All identity checks are be kept up to date and retained for five years after the termination of the business relationship or five years from the date when the transaction was completed.

11.5 All records of identity check, SARs and supporting documentation will be handled in confidence, stored securely, and will be capable of being retrieved without undue delay.

## 12. TRAINING

12.1 All employees which may be affected by this Policy will be provided with training on the law relating to money laundering and terrorist financing and any requirements relating to data protection.

12.2 All personnel are expected to be familiar with our anti-money laundering procedures. Attendance at training sessions will be monitored to ensure compliance with our anti-money laundering obligations.

12.3 The MLRO is responsible for ensuring that the Company's employees understand this Policy. The MLRO shall ensure that each employee confirms their understanding of this Policy (and related documents) by signing the table provided in Annex 3 of this Policy.

12.4 Employees are also trained on how to identify and deal with transactions that may be related to money laundering.

12.5 If you do not understand any of our anti-money laundering procedures or feel that you would like additional training, you should consult with the MLRO.

| | |
|---|---|
| **POLICY OWNER** | The Company owns this Policy |
| **APPROVAL** | This Policy has been approved by the Board of the Company |
| **IMPLEMENTATION** | The MLRO is responsible for ensuring that the Company's governance structures and procedures are adequate to meet the requirements of this Policy |
| **DATE APPROVED** | MARCH 2023 |
| **EFFECTIVE DATE** | MARCH 2023 |

## ANNEX 1 – SUSPICIOUS ACTIVITY REPORT

**YOUR DETAILS:**

| | |
|---|---|
| Your Name: | |
| Date of submission to the MLRO: | |
| Signature: | |

**DETAILS RELATING TO THE MAIN PERSON OR CORPORATION/PARTNERSHIP/TRUST TO WHICH THE SUSPICION RELATES:**

| | |
|---|---|
| Title: | |
| Surname: | |
| Forenames: | |
| Date of Birth: | |
| Gender: | |
| Nationality: | |
| Passport No: | |
| Occupation: | |
| Home Address:<br>(including postcode & country) | |
| Email address: | |
| Phone Number: | |
| Employer (where relevant): | |

**DETAILS REQUIRED IN RESPECT OF A COMPANY/PARTNERSHIP/TRUST:**

| | |
|---|---|
| Firm Name: | |
| Type of Business: | |
| Address:<br>(including postcode and country) | |
| Firm No: | |
| VAT No: | |

| Identities of any other person(s) known to be involved in the transaction(s): |
| --- |
| |

| Description of the transaction: |
| --- |
| |

| Capacity in which the person(s) known to be involved in the transaction(s): |
| --- |
| |
| Reason(s) for suspicion (please use a new page if necessary): |
| |

| Further information which may be of significance (please list any accompanying material you are supplying): |
|---|
| |

**PLEASE SIGN, DATE AND TAKE A COPY OF THIS REPORT FOR YOUR RECORDS PRIOR TO PROVIDING IT TO THE MLRO.**

| **FOR MLRO RECORDS ONLY:** | | Reference No: | |
|---|---|---|---|
| Date suspicion received: | | Date receipt provided for Suspicious Transaction Report: | |
| Reported to National Crime Agency (NCA): | Yes / No | Date reported to NCA: | |
| Response received from NCA: | Yes / No | Date of response from NCA: | |

## ANNEX 2 – SUSPICIOUS ACTIVITY REPORT LOG

| Reference number: | Date received: | Reported to NCA (Y/N): | Date reported to NCA | Response received from NCA (Y/N): | Date response received from NCA: |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## ANNEX 3 – CONFIRMATION OF EMPLOYEES UNDERSTANDING OF THE AML POLICY

| No. | Name and surname of employee | Employee's position | Date of acquaintance | Employee's signature |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |
| 12 | | | | |
| 13 | | | | |
| 14 | | | | |
| 15 | | | | |
| 16 | | | | |
| 17 | | | | |
| 18 | | | | |
| 19 | | | | |
| 20 | | | | |