ANTI-MONEY LAUNDERING & ANTI-TERRORISM FINANCING POLICY

TABLE OF CONTENTS

1.0 ABBREVIATIONS & DEFINITIONS

AML – Anti-money laundering

AMLATFA – Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613)

ATF – Anti-terrorism financing

BNM – Bank Negara Malaysia

CCC – Corporate Compliance & Control

CDD – Counterparty Due Diligence

Company - Carimin Petroleum Berhad and its subsidiaries

Compliance – Corporate Compliance & Control

Employee – any employee of the Company and shall include contract personnel, temporary staff, trainees and interns.

FATF – Financial Action Task Force

Head – CCC – Head of Corporate Compliance & Control

HRD – Human Resource Department

Management/Key Officers – Head of Business Units/Subsidiaries, HODs and senior executives of the Company who has privy to price sensitive information in relation to the Company

MCCG – Malaysian Code on Corporate Governance

ML/TF – Money Laundering / Terrorism Financing

MMLR – Main Market Listing Rules

OFAC – Office of Foreign Assets Control of the US Department of the Treasury

RBA – Risk-based Approach

SC – Securities Commission Malaysia

STR – Suspicious Transaction Report

UNSC – United Nations Security Council

2.0 PURPOSE

The purpose of this document is to advise all employees regarding **anti-money laundering (AML)** and **anti-terrorism financing (ATF);** and to provide guidance on preventing any involvement in such activities in line with the **Anti-**

Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFA).

This document provides information on the Company's policy regarding the matter.

This policy is intended to achieve the following objectives:

(a) To ensure that all employees are aware that money laundering and terrorism financing are serious offences and the repercussions of such breaches.
(b) To highlight the Company's concern and commitment towards AML and ATF governance.
(c) Compliance with the laws and regulations of Malaysia and those of other countries where we may have operations. Within Malaysia, we shall comply with the AMLATFA and the Securities Commission's Malaysian Code on Corporate Governance (MCCG).

3.0 SCOPE

This policy covers money laundering (ML) and terrorism financing (TF) including its definition, how it may occur, legal implications and consequences, and the Company's action to prevent these from occurring.

The policy applies to all business entities owned by the Company and to all directors, officers and employees. Wherever applicable, this policy may apply to contractors, vendors, service providers, advisors, consultants and other third parties acting on behalf of the Company.

4.0 REFERENCES

This policy shall be read and applied in conjunction with the following laws, regulations, policies and SOPs.

4.1 Relevant legal and regulatory requirements:

a) Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613)
b) Central Bank of Malaysia Act 2009 Act 701
c) Penal Code Act 574
d) Securities Commission Malaysia Act 1993 (Act 498)
e) SC's Guidelines on Prevention of Money Laundering Terrorism Financing
f) SC's Malaysian Code on Corporate Governance (MCCG)
g) Financial Action Task Force (FATF) Recommendations

4.2 Company Policies and Procedures:

a) Code of Conduct and Business Ethics (CG-HRA-OD-05)
b) Risk Management Policy & Framework (CG-CCC-RMPF-01)

5.0 POLICY STATEMENT

Company is committed to comply with all laws and regulations pertaining to money laundering, terrorism financing and proceeds of unlawful activities, in particular, the **Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613)**.

Company prohibits all practices or involvement related to money laundering, terrorism financing or proceeds of unlawful activities either directly or indirectly. We will cooperate with law enforcement agencies whenever necessary and disclose information as required.

A **risk-based approach (RBA)** shall be taken to identify, assess, monitor, manage and mitigate ML/TF risks as appropriate. These will be carried out commensurate with the nature, scale and complexity of our business activities or processes.

The Company shall from time to time perform **ML/TF risk assessments** and put into place appropriate **AML/ATF controls** to prevent the occurrence of such activities. We shall also provide training to employees to ensure that they are aware of these and be updated on any AMLATFA developments.

We will conduct reasonable and appropriate **Counterparty Due Diligence** (CDD) to understand the business and background of our prospective clients, vendors, third party or business partners.

The Company shall not have business ties and shall also not make payments, contributions or donations to individuals, corporations or organizations which are on **BNM, UNSC or OFAC sanctions listings.**

Any suspected activities or red flags must be reported to the Company's Corporate Compliance & Control (CCC) Department. CCC will evaluate the case and if confirmed shall submit a **Suspicious Transaction Report** (STR) to the relevant authorities.

For Company Directors, they shall report any ML/TF concerns to the Head - CCC for further action.

All employees shall abide by this policy and avoid any suspicious transactions.

6.0 WHAT IS MONEY LAUNDERING & TERRORISM FINANCING?

Based on Guidelines on Prevention of Money Laundering and Terrorism Financing issued by the SC, we can describe these as follows:

(a) Money Laundering

This generally involves proceeds of unlawful activities or "dirty money" which is processed or transformed through a series of transactions so that they appear to be "clean' funds from legitimate sources. Thus, the funds are "laundered".

The process of money laundering where funds usually go through three stages:

(1) **Placement** – where illegal funds are introduced into the financial system;

(2) **Layering** – where the funds go through many layers of transactions to distance or separate these funds from their sources and to disguise the audit trail; and

(3) **Integration** – where integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds.

(b) Terrorism Financing

This is the act of providing funds or property, whether legitimate or illegitimate, to support terrorists or terrorist organizations which assist or enable them to carry out terrorist acts.

Section 3(1) of AMLATFA defines a "terrorism financing offence" as any offence under Section 130N, 130O, 130P or 130Q of the Malaysian Penal Code Act 574, which are essentially the following:
(1) Providing or collecting property for terrorist acts;
(2) Providing services for terrorism purposes;
(3) Arranging for retention or control of terrorist property; or
(4) Dealing with terrorist property.

7.0 CONSEQUENCES OF BREACH & RISKS

Any employee who breaches this policy or the applicable laws, rules, regulations or code will be subject to disciplinary action, up to and including termination of employment. The employee involved in the breach may be subject to civil action and/or criminal action.

Violations may lead to extensive and costly investigations and incur legal expenses. Such acts may also result in serious repercussions to the Company such as fines or penalties and cause damage to the Company's reputation or brand name. It may also result in restrictions to our business operations or loss of licenses.

8.0 COUNTERPARTY DUE DILIGENCE

In general, all business units and departments are required to perform Counterparty Due Diligence (CDD) during the following:

(a) Prior to starting a new business relationship or making any contributions/donations;
(b) When reviewing the Counterparty status i.e. after several years of doing business; or
(c) Whenever there is a need for more information or if there is any suspicion of ML/TF activities.

Employees shall collect and review documentation from prospective or current clients, business partners, vendors, contractors, service providers including agents, consultants and others such as sports, social or charitable organizations. The information to be gathered include the following:

(1) Identity or incorporation / registration with supporting documents;
(2) Licenses, permits or approvals from Ministries, Agencies or Authorities;
(3) Corporate Profile or Website information;
(4) Identities of Board members, senior management or Patrons and Committee members in the case of charitable bodies/associations; and.
(5) Where applicable, Ethical and Integrity related policies/procedures such as its Code of Conduct and Business Ethics, Anti-Bribery & Anti-Corruption Policy and AML/CTF Policy

The information and documentation will be processed for ML/TF risks by assessing the Counterparty's background and the way it conducts its business or operations.

These shall be reviewed and assessed to ensure that we are working together with legitimate parties involved in lawful activities and that their funds are from lawful

sources. Counterparties must be free from any legal restrictions or sanctions and must not be on BNM, UNSC, OFAC sanctions listings.

9.0 RECORD KEEPING AND RETENTION

We shall keep records of all counterparties and the related transactions including:
(a) Agreements and contracts
(b) CDD documentation, reviews and risk assessments
(c) Business correspondence or communications
(d) Client and Vendor registers, accounts and statements
(e) Payment records

These shall be maintained and updated as necessary and retained for at least seven (7) years.

10.0 REPORTING RED FLAGS & SUSPICIOUS TRANSACTIONS

Employees shall take reasonable and appropriate steps to detect unacceptable, suspicious or illegal payments and transactions or "**red flags**".

Examples of red flags include the following:
(a) A client or counterparty who provide inadequate documentation, false or suspicious information; or appears to be reluctant to provide required information.
(b) Unusual payment requests – such as to a third-party bank account, large payments in cash or cash equivalent, or payment in a different currency than the one agreed upon.
(c) Receiving payments which are suspicious – such as large payments in cash, or payments from a third-party (unrelated to the contract), or payments from another country unrelated to the Client, or large over-payments which then require refunding.
(d) Requests to channel funds from one party via our company accounts to another third party for whatever reason.
(e) Contracts, job orders or purchases which are not consistent with the Client's business.
(f) Payments to or from countries with high risk for ML/TF and illegal businesses.
(g) Payments to or from countries which are considered as tax havens or offshore financial centres.

Whenever red flags, suspicious or illegal transactions are identified, these must be reported to CCC.

Each report will be evaluated by Head - CCC and if necessary, the concern shall be notified to the Managing Director. Any credible or substantiated concern shall subsequently be reported as an STR with the relevant Agencies or Authorities.

11.0 COMPLIANCE CONTROLS & EMPLOYEE RESPONSIBILITY

Senior management, heads of departments and managers are responsible for compliance with this Policy and to ensure that there are appropriate and effective controls in place to prevent, detect and respond to ML/TF issues.

They shall communicate the Policy and cascade the information to all employees especially regarding the serious consequences of non-compliance.

CCC shall update employees on legislation developments and provide training on AMLATFA matters together with HRD.

Every employee has the responsibility to read and comply with this Policy and to report any red flags, suspicious or illegal transactions to Head – CCC.

12.0 BOARD APPROVAL

This Policy was reviewed and approved by the Board of Directors of the Company on 24th August, 2022.