CleanMax™
POWERING SUSTAINABILITY

Clean Max Enviro Energy Solutions Limited

Anti Money Laundering and Trade Sanctions Policy

August 2025

Description	The Policy is to provide rules and guidelines to be adopted and followed by Clean Max Enviro Energy Solutions Limited and it its subsidiaries and joint ventures and its intra-group entities ("**Company"** or "**CMES"**) its employees, and any third-party contractors appointed by the Company (to the extent as set out in this document).

Versions and History

Version	Date	Summary of Changes
1.0	25 May 2023	Version 1

I. Introduction

Clean Max Enviro Energy Solutions Limited ("**Company**") adopts the Anti-Money Laundering ("**AML**")[1] and Trade Sanctions Policy ("**Policy**"). This Policy shall apply to all directors, officers, employees and temporary workers[2] and shall be read in conjunction with the Company's Code of Business Conduct and Ethics.

This Policy has been approved by the board of directors ("**Board**") at its meeting held on 25 May 2023.

This Policy shall come into force with effect on the date on which the Board approves this Policy.

II. Zero Tolerance Approach to Money Laundering and Trade Sanctions Noncompliance

The Company has built a reputation for conducting business with honesty and integrity. Maintaining this reputation is essential to preserve the trust and ensure confidence in its business by customers, clients, investors and other persons. It is integral to the Company's business that it promotes a zero-tolerance approach towards financial crime and accordingly, it is committed to not being involved in, or otherwise facilitating, financial crimes of any kind.

Money laundering shall mean the process of disguising the true source of illegally obtained funds, usually by integrating the funds into otherwise legitimate businesses or transferring the funds through a series of complex financial transactions ("**Money Laundering**"). The proceeds of illegal activities such as bribery or corruption are often disguised through Money Laundering.

For the purposes of this Policy, references to Money Laundering, shall also include terrorist financing, which refers to the use of money to support terrorist activities, irrespective of how such funds are obtained.

The Company shall be required to comply with laws and regulations in the countries where it operates / conducts business. These regulations include a list of restricted individuals, entities, and countries with whom business transactions are prohibited or limited. As a result, the Company shall comply with these requirements and ensure that it does not engage in business with any such restricted counterparties.

Certain regulations require the Company to implement systems and controls to identify, assess, monitor, and manage risks related to Money Laundering and trade sanctions. Failure to adequately establish and implement risk-based systems may result in regulatory penalties or legal action for non-compliance with financial crime prevention regulations/ requirements.

III. Know-Your-Counterparty

A key aspect in mitigating potential Money Laundering and trade sanctions risks is to know-your-counterparty ("**KYC**"). In this regard, the Company shall adopt a risk-based approach to due diligence and KYC. Where deemed appropriate, due diligence shall be undertaken on counterparties prior to investment or divestment transactions (including but not limited to, the purchase or sale of a portfolio company), joint venture partnerships and prior to engaging in other third-party relationships. In ongoing relationships, counterparties shall also be monitored based on the risk for any suspicious activities or transactions.

The Company shall establish procedures outlining the specific due diligence measures to be followed, which may vary depending on the nature of the counterparty relationship that is involved. In all instances,

[1] For purposes of the Policy, anti-money laundering includes counter terrorist financing.

[2] For purposes of the Policy, "temporary workers" include non-full-time employees and consultants and contractors, etc. that work on the Company's premises. The business group retaining a temporary worker is responsible for ensuring that the temporary workers certifies their commitment to comply with this Policy.

these procedures shall require the collection of documentation to verify the counterparty's identity and to assist in a preliminary risk assessment. Based on the outcome of this risk assessment, additional and enhanced due diligence may be necessary before deciding to engage with the third-party or proceed with the transaction. The procedures also outline mitigation measures tailored to the specific risks identified, along with ongoing monitoring obligations.

The risks to be considered include, but are not limited to:

i. Whether the counterparty/business is located in a high-risk jurisdiction with respect to Money Laundering;

ii. Whether the counterparty/business operates in an industry with heightened risks of Money Laundering, or is based in a sanctioned country;

iii. Whether the counterparty/business has any associations or connections with public officials or other political exposures; and

iv. Whether there are known reputational concerns or other issues involving AML exposure.

As outlined in the due diligence procedures, proper documentation shall be maintained for all due diligence activities conducted.

For further details, individuals are requested to refer to the Company's Anti-Money Laundering Transaction Procedures

IV. Investor KYC

The Company shall engage third-party fund administrators to collect certain minimum identification information from each new investor. These administrators shall utilize risk-based measures to verify both investor identities and document, the investor identification information and the verification methods and results, in accordance with their applicable administrator's AML protocol. This includes collection of all necessary documents and information required for identification and verification purposes of the prospective investors.

V. Monitoring

Ongoing relationships with counterparties shall require varying degrees of AML monitoring, including screening for changes in the counterparty's risk profile, particularly in connection with specific transactions or other activities which involve the counterparty. Appropriate KYC measures shall be considered whenever material changes to the counterparty are identified. Such changes shall include, but are not limited to, changes in location or address involving a high-risk jurisdiction, changes in ownership or control of an entity or bank account, or any other circumstances, in which considerations relevant to the Company's original risk assessment have materially changed. Records of the ongoing monitoring process shall be properly maintained.

VI. Trade Sanctions

Trade sanctions are economic, financial, trade or other restrictive measures imposed by individual countries, groups of countries, or multilateral organisations, such as the United Kingdom (UK) government, the United States (U.S.) government, the United Nations (UN) and the European Union (EU), on targeted regimes, countries or regions, governments, entities or individuals ("**Sanctions Target**").

These measures aim to achieve specific foreign policy or national security objectives.

These restrictions can be in the form of measures imposed directly against the Sanctions Target or restrictions on the ability of other persons to deal with, or on behalf of, the Sanctions Target. Types of sanctions may include:

i. Trade sanctions, including restrictions on providing services and/or maintaining relationships with Sanctions Targets, arms embargoes and restrictions on dual-use items;

ii. Financial sanctions, including asset freezes; and

iii. Immigration sanctions (also referred to as travel bans).

The Company is legally obligated to comply with applicable sanctions restrictions in the jurisdictions where it operates, as well as jurisdictions like the United States of America where such laws have extra-territorial application.

The Company shall not enter into any sort of business relationship with individuals or entities that are a Sanctions Target or otherwise subject to sanctions restrictions (depending on the scope of relevant trade sanctions), including country or region-wide restrictions. As a part of its due diligence process, counterparties shall be screened against sanctions, financial crime and adverse media watch lists. These screenings shall include:

i. The UN "**Consolidated Sanctions List**";

ii. The EU "**Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions**";

iii. HM Treasury (HMT), Office of Financial Sanctions Implementation (OFSI) "**Consolidated List of Targets**";

iv. The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) "**Specially Designated Persons and Blocked Persons List**"; and

v. The U.S. Commerce Department's Bureau of Industry and Security "**Entity List**."

Where a potential positive match is identified, a representative of the Company's Legal and Regulatory team shall be notified immediately.

VII. Reporting of Suspicious Activity and Transactions

Employees are / shall be obligated to report any suspicious transactions or activities to their Finance Controller or equivalent listed as a key contact as provided in Section VIII of this Policy. Once the employee has filed an internal report relating to the suspicious activity, the Finance Controller shall review the case and determine the appropriate course of action to take. This may include filing a Suspicious Activity Report ("**SAR**") with the reporting authority in the relevant jurisdiction. Care must be taken to ensure that the person or third party who is the subject of a suspicious report is not made aware of (or "tipped off" relating to) a disclosure having been made to a nominated officer or the reporting authority, as this may constitute a criminal offence in some jurisdictions where the Company operates.

VIII. Key Contacts

If you have any questions on this Policy, please contact:

Finance Controller: Sushant Nagre
Mail: suhant.nagre@cleanmax.com
Phone: +91 9867794469

General Counsel- Sanjay Bhatia
Mail: Sanjay.bhatia@cleanmax.com
Phone: +91-8754502793