



ANTI-MONEY LAUNDERING POLICY



1. INTRODUCTION

- 1.1. This anti-money laundering policy ("**Policy**") is devised and implemented in furtherance of the good corporate governance practice of TruAlt Bioenergy Limited ("**TruAlt**" or "**Company**") and to combat the risk of money laundering and terrorist financing. The Government of India, including the sectoral controllers and the regulatory authorities, have conveyed significant concerns over money laundering activities from time to time, which are illegal and anti-national. The Company's major presence in its respective industry and being an institutional participant in its respective trade, the Company deems it critical that strict and vigilant monitoring of suspicious activities is maintained by way of this Policy and the processes stated herein.
- 1.2. Compliance with the provisions of this Policy is mandatory. If a local law or business unit imposes stricter requirements than those described in the Policy, the more stringent of the two must be adhered to. The anti-money laundering laws applicable on the Company includes the (Indian) Prevention of Money-Laundering Act, 2002 ("**Act**") and all other applicable economic laws and regulation in the applicable jurisdictions.

2. PURPOSE

- 2.1 This Policy applies to the Company and its employees, vendors, business partners, suppliers, contractors, consultants, agents and representatives ("**Company Associates**"), to ensure that the Company is in compliance with all the applicable anti-money laundering laws.
- 2.2 The Company understands that the measures against money laundering and terrorist financing is a universal priority, and that these measures are a team effort, which does not only include the key officials of the Company, but each and every personnel of the Company.
- 2.3 The Company ensures that its policies, including this Policy, procedures, systems, methodologies, routine limit tests and audits appropriately and adequately address the requirements under the Act and the rules framed thereunder, including other applicable laws.
- 2.4 The primary purpose of this Policy is to prevent, mitigate and to keep in check any involvement of activities related to money laundering whether directly or indirectly, whether intentional or not, in the conduct of the operations and business activities of the Company.
- 2.5 This Policy mandates the Company Associates to recognize and report questionable financial transactions.

3. SCOPE

- 3.1 The Company is committed to carrying on its business activities with the highest ethical standards and thereby ensures strict compliance with the anti-money laundering laws.
- 3.2 This Policy is applicable to all the Company Associates. The Policy has been adopted at a meeting of the Board of Directors of the Company held on 3rd May 2024.

4. MONEY LAUNDERING

- 4.1. In general terms, 'money laundering' may be defined as the act of cleansing of money, that is money obtained illegally or through illegitimate non *bona-fide* activities, which include, without limitation, drug trafficking, terrorism, organized crime, fraud, cartels and/or other activities of equivalent nature, wherein such activities are carried out in hiding, generating illegal money and such money is used in a legally usable form. The hidden and illegal activities then are disguised as legal activities through which the money that is generated, thereby attempting to legitimise such money.
- 4.2. The Act defines the offence of money laundering as "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money laundering."
- 4.3. Money laundering usually involves three steps: (i) Placement; (ii) Layering; and (iii) Integration. Placement, being the first step, involves the generation of money through illegal activities and thereafter, such money is attempted to be disposed of and converted into legally accepted forms, such as money orders, cheques, etc. Layering involves a process wherein the funds are rounded into multiple transactions in an effort to hide their origin and separate such funds from the illegal activities through which it was generated/obtained. The multiple transactions create a layer wherein the movement of funds is between multiple accounts, businesses involving buying and selling assets on a local or an international basis and thereafter, the origin of such funds become virtually untraceable. Integration occurs when the funds, which are layered and are successfully introduced into the financial system, are reintroduced into the economy and are often used to purchase legitimate assets, fund legitimate businesses or their equivalent.

5. PROCEDURES AND CONTROLS

5.1. Identification & Reporting

- (a) The Company ensures that sufficient background checks and diligences are carried out to assess and mitigate the potential anti-money laundering (AML) risks, which include, without limitation, verifying third-party's identity (for individuals, this can include requesting a copy of their passport or other national identification documents such as Aadhaar Card, PAN Card, Voter ID Card, etc.) in consonance with the applicable laws.
- (b) In furtherance to the identification procedure above, the Company will be extra cautious with the entities/individuals who are reluctant to provide the necessary information for identification/background check purposes. Similarly, (i) entities/individuals who are acting as an agent of a third-party and refuse to divulge necessary information of such third party, or (ii) entities/individuals who do not want to record the transaction or avoid the record-keeping of essential documents, or (iii) entities/individuals who only want to conduct business activities in cash to avoid an electronic trail of the transaction or (iv) entities/individuals who, against their ordinary course business, submits a much larger purchase order vis-à-vis complex payment structure which does not involve any economic sense, or (v) entities/individuals requesting payments to be made to a third-party who is

unrelated to the transaction in every sense, or (vi) entities/individuals facilitating partial payments in multiple tranches from different third-parties/sources, or (vii) entities/individuals whose business address is not a physical site, or (viii) entities/individuals making the payment through one medium and collects payment/refund through another medium, are made subject to comprehensive verification process.

- (c) The Company has set-up a 'Know Your Customer'/'Customer Identification Procedure' to effectively implement the identification procedure of the Company's business partners, suppliers, customers, vendors etc.
- (d) The relevant Company officials, who may be handling different third-parties, as part of the Company's business activities are to strictly report any unusual behavior, requests, payments, etc. to the Company's compliance team, as may be designated by the board of directors ("**Board**") of the Company, from time to time, and the compliance team shall immediately instruct to stop such engagement until further notice.
- (e) In the event the reporting to the compliance team takes time, which may be due to business exigencies, then such personnel/employee shall report the abovementioned activities to their immediate supervisor/manager urgently.

5.2. Roles & Responsibilities

- (a) The Company's compliance team will oversee the implementation and exercise of this Policy.
- (b) The Board shall not criticize any employee or its directors/employees for any loss of business resulting from adherence of this Policy.
- (c) The Company Associates who are engaging with the customers, vendors and suppliers on a day-to-day are to be trained to be mindful of this Policy and carry out their duties in this regard.
- (d) The Company Associates are responsible for maintaining strict protocols in terms of engaging communication with the third-parties, have appropriate written records to execute the business activities and have requisite approvals in terms of consummating transactions.

5.3. Retention of Records

- (a) While the applicable laws mandate maintenance of records of the business activities of the Company, as per this Policy, every Company Associate is mandated to maintain records of each transaction, related documents, identification records, communication records, etc. at all times.
- (b) The periodic audits that are carried out by the Company and the training given to the Company Associates shall ensure that such measures are implemented and maintained at all times without failure.

5.4. Financial Intelligence Unit – India

- (a) Financial Intelligence Unit – India (“**FIU-IND**”) is the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions to enforcement agencies and foreign FIUs. It functions solely to safeguard India’s financial system from the adverse impact of money laundering, terrorist financing and other economic crimes.
- (b) Core functions of FIU-IND include:
- i. Collection of information from reporting entities, which includes the Company;
 - ii. Analysis of information to uncover money laundering/terrorist financing;
 - iii. Sharing of information with the law enforcement and foreign financial intelligence units;
 - iv. Acting as a central repository;
 - v. Co-ordinating the fight against money laundering/terrorist financing; and
 - vi. Conducting research and analysis for money laundering/terrorist financing trends and typologies.
- (c) With the introduction of FINGate 2.0 (*available at fingate.gov.in*), the Company is to periodically keeps track of any directions/guidelines that may be published, pertaining to money laundering/terrorist financing, by FIU-IND and subsequently is to ensure to include as a part of its training within the organization.

5.5. AML Risks

- (a) Violation of the Act and other applicable laws, including this Policy, may, in respect of the defaulting person/entity (which could include the Company), lead to (as applicable):
- i. severe civil and/or criminal penalties against the concerned organizations;
 - ii. significant monetary fines;
 - iii. imprisonment;
 - iv. extradition;
 - v. blacklisting;
 - vi. revocation of license;
 - vii. disqualification of directors;
 - viii. loss of reputation;
 - ix. practical consequences in terms of commercial relationships and business partnerships;
 - x. restrictions;
 - xi. surveillance; and
 - xii. extensive time and cost investment in conducting investigations, etc.
- (b) While the Company is aware of the risks associated in this regard, the Company shall ensure that there is no stone left unturned, on account of the Company, to implement and maintain the exercises, protocols, measures and intention as outlined in this Policy by way of periodic audits by the Company and periodic trainings to the personnel/employees/staff/consultants/agents, etc.

5.6. Red Flag Checklist

- (a) Apart from the KYC procedure , which outlines the extensive steps prior to onboarding a new customer/supplier/vendor/service provider and extensive steps to ensure that all the data and records are accurate as of date, this Policy outlines the red flag checklist, which are the specific matters to be checked, in relation to money laundering/terrorist financing.
- (b) The following checklist should be ticked off at all times in the event the Company is engaging with such third-party for any reason, whatsoever:
 - i. obtain sufficient information to identify persons who beneficially own or control the third-party, as the case may be;
 - ii. verify the third-party's identity using reliable, independent source documents, data or information to ensure that the third-party with whom the Company is entering into a business relationship is actually the third-party as represented;
 - iii. approved third-parties shall periodically update all documents, data or information on a periodic basis, as may be determined by the Board;
 - iv. the personnel/employee or some key personnel/official who is undertaking the business relationship should attempt to meet the third-party in person;
 - v. conduct sufficient background checks to ensure that the third-party is not blacklisted or sanctioned, has a history of successful and *bona-fide* business activities and relationships, etc.;
 - vi. ensure that the third-parties adhere to the KYC procedure
 - vii. do not accept third-parties who have relationships with or have criminal backgrounds or history;
 - viii. ensure that the third-parties are not fictitious entities and that they have a valid license in terms of existence of the entity and to conduct its business activities;
 - ix. if required, to conduct a visit of the third-party's premises/site of operation and to ensure that such premises/site has been in operation since a good amount of time; and
 - x. any other measure that may be prescribed under this Policy or stipulated by the Board.

5.7. Training / Recruitment

- a) The Company will ensure that, at the time of recruitment/engagement, appropriate background checks are conducted to ensure that the individual/entity who is getting hired/engaged has a clean history without any criminal associations or association with any of the blacklisted entity(ies).
- b) The Company will periodically train the Company Associates in light of this Policy to keep the Company Associates apprised of the significance of AML protocols, including any latest developments thereto. The training also includes the steps to be taken while interacting with a third-party and is mandated that all communication should be on record.
- c) In addition to the above, the training covers (i) the AML definition, guidelines and requirements, (ii) AML risks due to non-compliance of this Policy, (iii) prevention of fraud or suspicious transactions, and (iv) mandatory documentation for AML.

5.8. Audit

- a) The Company will periodically set-up and conduct internal audits/inspections of every department/business to ensure compliance with the Company's policies, including this Policy, other procedures and controls relating to money laundering activities.
- b) In the event of non-compliance by any of the department/business, the Board will ensure that such department/business undertakes appropriate steps and measures to rectify the same, in accordance with this Policy.

5.9. Review

The Board will undertake a review of this Policy periodically to ensure that the guidelines/directions that are mentioned herein are at par with the current legislation's requirements and in accordance with the guidelines/directions as may be published by the Government of India or any other applicable jurisdiction.

6. VIOLATION AND CONSEQUENCES

6.1. Violations

Any violation of the provisions set forth under the Act or a violation of this Policy shall amount to gross misconduct and contravention, and an indicative list of such violations is set-out below:

- i. violation of the objective of this Policy;
- ii. engaging a third-party without following the red flag checklist or other compliance steps;
- iii. influencing others to violate this Policy;
- iv. failure to report any violation or red flag under this Policy;
- v. failure to co-operate in the investigations under this Policy;
- vi. threatening/extorting other employees for complying with this Policy;
- vii. involvement in any money laundering/terrorist financing activities, whether in the course of employment of the Company or otherwise; and
- viii. any other violation, as may be decided by the Board at its discretion.

6.2. Consequences of Violation

- i. *Corrective Action:* The Board or the Company's compliance team may prescribe corrective actions in line with this Policy; and/or
- ii. *Penalties:* The Board or the Company's compliance team, based on the investigations as may be conducted upon violation of this Policy or otherwise, may prescribe specific disciplinary actions, including suspension and/or termination of employment/engagement/service. Further, the Board or the Company's compliance team may penalize such individuals and/or commence civil/criminal proceedings against such individuals/entities under the applicable laws.

7. MONITORING AND REVIEW

- 7.1. Continuous Monitoring: TruAlt is committed to the continuous monitoring of its anti-money laundering efforts and measures. This includes monitoring the implementation of this Policy across all departments and locations to ensure compliance with its provisions.
- 7.2. Internal Audit: The Company's compliance team, in collaboration with the internal audit team, will conduct regular audits to assess the effectiveness of the anti-money laundering controls and procedures. These audits will help identify any gaps in compliance and areas for improvement.
- 7.3. Risk-Based Approach: TruAlt will adopt a risk-based approach to monitoring and review, focusing its efforts on high-risk areas and third-party relationships. This approach will help prioritize resources and ensure that the most significant risks are addressed promptly.
- 7.4. Feedback Mechanism: TruAlt encourages feedback from the Company Associates regarding the effectiveness of this Policy and its implementation. The Company Associates are encouraged to report any concerns or suggestions for improvement through the established reporting mechanisms.
- 7.5. Reporting to the Board: The findings from the monitoring and review process will be reported to the Board. This report will include an overview of the Company's anti-money laundering efforts and procedures, any identified areas of non-compliance, and recommendations for improvement.
- 7.6. Adjustments to the Policy: Based on the findings from the monitoring and review process, TruAlt will make necessary adjustments to this Policy and related procedures. These adjustments will be aimed at strengthening the Company's anti-money laundering framework and ensuring its continued effectiveness.
- 7.7. External Review: TruAlt may engage external auditors or consultants to conduct periodic reviews of its anti-money laundering efforts and procedures. These external reviews will provide an independent assessment of the Company's compliance with this Policy and relevant laws and regulations.
- 7.8. Training and Awareness: The monitoring and review process will also assess the effectiveness of the training programs and awareness campaigns related to anti-money laundering. Any necessary adjustments to these programs will be made to ensure they remain relevant and impactful.

8. POLICY GOVERNANCE

- 8.1. Governance and Oversight: The Board is committed to upholding the highest standards of corporate governance and ethical conduct. The Board recognizes its role in overseeing the implementation of this Policy and ensuring that it aligns with the Company's values, ethical standards and legal obligations.
- 8.2. Setting the Tone: The Board is responsible for setting the tone at the top and establishing a culture of integrity and transparency throughout the organization. It ensures that this Policy remains dynamic and responsive to the ever-changing landscape of global business and international anti-money laundering norms.
- 8.3. Policy Review and Update: The Board oversees the regular review and update of this Policy to ensure its effectiveness in addressing the risks associated with money laundering.
- 8.4. Resource Allocation: The Board shall ensure that appropriate resources are allocated for the implementation of this Policy, including training programs, monitoring mechanisms and reporting procedures. It shall monitor the effectiveness of these resources and make adjustments as necessary to ensure compliance with this Policy.
- 8.5. Commitment to Integrity: Overall, the Board plays a crucial role in ensuring that TruAlt conducts its business with integrity, transparency and fairness. The Company is committed to upholding the highest standards of corporate governance and ethical conduct and will take all necessary steps to prevent and detect money laundering in the Company's operations.

