

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 1 of 14



Corporate Anti-Money Laundering

and

Counter-Terrorist Financing Compliance Manual

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 2 of 14



Prepared by: _____

Date: 22nd of April 2020

(by Markus Ganterer, CFO)

Reviewed by: _____

Date: 22nd of April 2020

(by Pankaj Ghai, Director)

Approved by the board of directors:

Date: 22nd of April 2020

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 3 of 14

Amendment record

Revision	Effective date	Nature of change
0	22 nd April 2020	Initial issue

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 4 of 14



Table of Contents

I. Objective 5

II. Scope and Applicability 5

III. Policy Details 5

 III.1 General 5

 III.2 Applicable Legislation..... 7

IV. Requirements..... 8

 IV.1 General Requirements and Commitments 8

 IV.2 Record Keeping & Reporting Requirements..... 12

V. Administration of the Policy 14

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 5 of 14

Corporate Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual

I. Objective

This policy outlines how Constant Energy Singapore Holding Pte. Ltd. (together with its subsidiaries, hereafter referred to as the “**Company**”), which operates in the solar energy sector, will prohibit and actively prevent money laundering and counter-terrorist financing both directly and indirectly through its business operations.

The Company is committed to the highest possible standards of conduct and has, therefore, put in place appropriate and proportionate anti-money laundering (**AML**) and counter-terrorist financing (**CTF**) safeguards and reporting arrangements. To re-affirm this approach, the Board has adopted this written policy to which sets out the detailed guidelines for business activities which will avoid AML and CTF.

II. Scope and Applicability

This policy applies to all the Company’s business activities, all shareholders (including ultimate beneficial owners and any interim holding companies) and employees of the Company, including officers, directors and other staff, whether permanent, temporary or contract workers, and all persons acting on behalf of the Company (collectively, the “**Employees**”).

The aim of the policy is to enable the Employees to respond to a concern they have during their dealings for the Company. Individuals who have a concern relating to a matter outside of work should contact the Police.

III. Policy Details

III.1 General

Money laundering is generally described as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Examples of money laundering acts include the following:

- Participating directly or indirectly in financial, banking or another transaction in order to conceal the illegal origin of money or property which is acquired from commission of a crime;
- Using money or property which is acquired from commission of a crime for business or other activities;
- Concealing information about the origin, true nature, location, movement or ownership of money or property which is acquired from commission of a crime, or obstructing the verification of such information;

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 6 of 14

- Committing one of the above-mentioned acts toward money or property which the person committing the acts knows, is acquired from the movement, transfer or conversion of money or property acquired from another person’s commission of a crime;
- Provision of assistance to any organization or individual involved in the crime in order to evade legal responsibilities by way of legalizing the source of assets obtained as a result of the crime; and
- Possession of assets if, at the time of receipt of such assets, it is thoroughly known that they were obtained as a result of the crime, in order to legalize the origin of the assets.

Generally, the process of money laundering comprises of three stages, which may involve numerous transactions:

- Placement – the physical disposal of cash proceeds derived from illegal activity;
- Layering – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity; and
- Integration – the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

Money laundering has commonly been associated with drug trafficking where drug proceeds are laundered through the financial system or other means. Other criminal activities often associated with money laundering are selling illegal arms, selling stolen goods, terrorist financing and human trafficking. Proceeds of crime relates to any property derived or obtained, directly or indirectly, by any natural person or entity (collectively, “**Person**”) as a result of criminal activity relating to a scheduled offence or value of such property.

Terrorism financing, on the other hand, is the provision or collection of funds for the support, advancement or perpetration of acts of terrorism. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 7 of 14

III.2 Applicable Legislation

The Company’s long-standing commitment to doing business with integrity means avoiding corruption in any form, including money laundering, bribery and financing terrorist activity, and complying with the applicable laws.

International standards of anti-money laundering and counter-terrorist financing are set by the Financial Action Task Force (FATF).

Singapore

As a member of the FATF, Singapore implements recommendations promulgated by this inter-government body to combat money laundering and terrorist financing.

The applicable legislation and guidelines concerning AML and CTF in Singapore are as follows:

- Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A) (**CDSA**); and
- Terrorism (Suppression of Financing) Act (Cap. 325) (**TSFA**).

Vietnam

Although Vietnam is not a member of the FATF, Vietnam is a member of the Asia/Pacific Group on Money Laundering (i.e., a FATF-Style Regional Body acknowledged by FATF), and Vietnam implements recommendations promulgated by this inter-government body to combat money laundering and terrorist financing.

The applicable legislation and guidelines concerning AML and CTF in Vietnam are as follows:

- Penal Code No. 100/2015/QH13 dated 27 November 2015 (as amended) and its implementing documents;
- Law on Anti-Money Laundering No. 07/2012/QH13 dated 18 June 2012 and its implementing documents; and
- Law on Anti-Terrorism No. 28/2013/QH13 dated 12 June 2013 and its implementing documents.

Thailand

Although Thailand is not a member of the FATF, Thailand is a member of the Asia/Pacific Group on Money Laundering (i.e., a FATF-Style Regional Body acknowledged by FATF), and Thailand implements recommendations promulgated by the FATF to combat money laundering and terrorist financing.

The applicable legislation and guidelines concerning AML and CTF in Thailand are as follows:

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 8 of 14

- Anti-Money Laundering Act, B.E. 2542 (1999) (as amended) and its implementing documents; and
- Terrorism and Proliferation of Weapons of Mass Destruction Financing Act, B.E. 2559 (2016) (as amended) and its implementing documents.

IV. Requirements

IV.1 General Requirements and Commitments

IV.1.1 The Company will carry out all business activities with applicable laws, including the laws of Vietnam, Thailand and Singapore.

IV.1.2 The Company and its Employees will not attempt to indulge or assist other person or actually involved in any activity connected with the proceeds of crime and projecting it as untainted property.

IV.1.3 The Company will ensure that all external, internal, direct or indirect transactions are documented at face value and follow company accounting procedures. Manipulation of accounts, expenses, sales/receipts/invoices will not be tolerated. All Company Employees must:

- Follow the Company’s accounting requirements as set out in the Company’s generally accepted accounting principles;
- Accurately record all transactions;
- Maintain accurate books and records, including records of payments to agents, consultants, representatives, third parties, and government officials in accordance with the Company’s generally accepted accounting principles;
- Never agree to requests for false invoices or for payment of expenses that are unusual, excessive, inadequately described, or otherwise raise questions under these guidelines; and
- Never make / receive any payments to anonymous (i.e., “numbered”) accounts that are in the name of neither the payee nor an entity known to be controlled by the payee.

IV.1.4 The Company will report any Employee that it has reasonable ground to believe has committed money laundering to the applicable government authority.

IV.1.5 The Company will not issue any equity interests to any Person that (a) is in any Restricted Country, (b) is subject to any Sanction, or (c) has any legal or beneficial owner (including the ultimate owner(s) and any interim companies) that is in any Restricted Country or is subject to any Sanction. For purposes of this policy,

“Restricted Country” means Iran, Cuba, North Korea, Syria or any other country or territory the government or nationals of which any Person subject to the jurisdiction of the United States is or becomes prohibited from dealing with under any Sanction administered by the United States

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 9 of 14

Department of the Treasury’s Office of Foreign Assets Control¹ or any other United States governmental authority); and

“**Sanctions**” means the “Specially Designated Nationals And Blocked Persons” list² maintained by the United States Department of the Treasury’s Office of Foreign Assets Control³, the World Bank Listing of Ineligible Firms⁴, the United Nations Security Council Sanctions Lists⁵, and any other publicly available internationally recognized “blacklist” or embargo program administered or imposed by any United States governmental authority, the World Bank Group, the United Nations Security Council (or its committees), the European Union (including the financial sanctions under the European Union Common Foreign and Security Policy⁶), Interpol, the Asian Development Bank⁷, or any governmental authorities of Vietnam, Thailand and/or Singapore⁸;

IV.1.6 The Company will not finance any terrorist activity, and will not accept or receive payments from high risk countries (i.e. those which have not implemented legislation bringing in to effect UN Sanctions, or those that are categorized as a “strategically deficient” jurisdiction by FATF in relation to AML/CTF⁹).

IV.1.7 The Company will not (and will ensure that the Employees will not) directly or indirectly have any asset in, make any sale to or engage in any business activity with or for the benefit of, or finance any activity of any Restricted Country, any country that is not a member of the International Finance Corporation¹⁰, or any other country or Person that is subject to any Sanction.

¹ The countries that are categorized as “Restricted Countries” due to OFAC-administered Sanctions can be found on the OFAC Sanctions list (same as in Footnote 4 above); but note that, as of July 1st, 2019, some of the countries on that list are not categorized as “Restricted Countries” (given how such term is defined in this policy).

² Specially Designated Nationals And Blocked Persons list (administered by the US Department of the Treasury’s Office of Foreign Assets Control (OFAC)) <<https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>>

³ OFAC Sanctions list <<https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>>

⁴ World Bank Listing of Ineligible Firms <<https://www.worldbank.org/en/projects-operations/procurement/debarred-firms>>

⁵ United Nations Security Council Sanctions Lists <<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>>

⁶ European Union Common Foreign and Security Policy Sanctions List <https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions>

⁷ ADB Sanctions List <<http://lnadbg4.adb.org/oga0009p.nsf/sancALLPublic?OpenView&count=999>>

⁸ Singapore’s approach to sanctions is to implement the United Nations Security Council sanctions, and to designate certain additional entities and individuals with whom dealings and transactions are subject to restrictions. For further information on the sanctions rules which non-financial institutions and natural persons in Singapore must comply with, please refer to <https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions>.

⁹ FATF, High-risk and non-cooperative jurisdictions <<http://www.fatf-gafi.org/countries/#high-risk>>

¹⁰ IFC member list <<http://www.worldbank.org/en/about/leadership/members#3>>

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 10 of 14

IV.1.8 Before establishing any business relationship with a third party client/customer or business partner, the Company will (and the respective Employees will) verify the identity of such third party as follows:

- (a) as to an individual, obtaining an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport (it being understood that medical cards, credit cards and student identification cards should not be accepted as the sole means of identification); the information to be verified include full name; date of birth; nationality, occupation and title, phone number (for nationals of Vietnam, Thailand or Singapore , ID card or passport number, date of issuance, place of issuance, visa (for foreigners); permanent residential address and current residential address (for nationals of Vietnam, Thailand or Singapore; or registered residential address overseas and registered residential address in Vietnam, Thailand or Singapore (for foreigners);
- (b) as to a person other than an individual, obtaining (i) a copy of its certificate of incorporation/formation and its constitutional documents (such as Articles of Incorporation and partnership agreements), and (ii) information about its full name and abbreviation; registered address and business address(es); phone number; fax number; business sectors; information of founders, representatives and ultimate beneficial owners (and any interim holding companies), in each case certified as complete and accurate by such person or its legal counsel; and
- (c) in each case, conducting such further risk-based verification and know your customer (KYC) procedures as may be necessary under the respective circumstances (including a search or inquiry with the relevant supervising authority/regulatory agency and enhanced due diligence for those customers presenting higher risk), understanding the source of payments by such third party and checking the Sanctions lists identified in 4.1.5.

The Company will not carry out any business transactions with any third party the identity of which cannot be confirmed. The Company will carry out additional due diligence if transactions are being made from overseas, particularly if any customers/clients of counterparties of the client a) reside or have a physical presence in; or b) undertake any commercial activities in countries or in sectors and/or entities referred to in the Sanctions lists identified in 4.1.5 or c) involve any individuals with political influence. The Company will also carry out additional due diligence on transactions involving new technology. The Company will also exercise due care in dealing with "shell companies," which, albeit being legal entities, have no business substance but through which financial transactions may be conducted, and, as such, are more likely to be used as conduits for money laundering activities.

All material information with respect to the Company's customers/clients and other key business partners shall be kept current and accurate through the conduct of regular verification and updates. The Company will document our verification, including all identifying information, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process.

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 11 of 14

IV.1.9 The Company will monitor account/payment activities for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to its business. The Company’s CFO and Legal Department will be responsible for this monitoring, will review any activity that the monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

(a) Customers/Clients/Business Partners – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.
- Reluctant to provide requisite identification documents.
- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.
- Background is questionable or differs from expectations based on business activities.

(b) Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an employee not to file required reports or not to maintain required records.
- Unusual concern with the Company’s compliance with government reporting requirements and firm’s AML policies.

(c) Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.
- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

(d) Other Suspicious Customer Activity

- Law enforcement subpoenas.
- Payment by third-party check or money transfer without an apparent connection to the customer.
- Payments to third-party without apparent connection to customer.
- No concern regarding the cost of transactions or fees (i.e., surrender fees, higher than necessary commissions, etc.).

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 12 of 14

When an Employee detects any red flag, or other activity that may be suspicious, he or she will notify the Company’s CFO and Legal Department. Under the direction of the CFO and Legal Department, the Company will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, and/or freezing the account.

IV.2 Record Keeping & Reporting Requirements

IV.2.1 The Company’s accounts will be maintained and retained for a minimum period applicable to each specific type of accounts documents in accordance with the regulations on accounting of Vietnam, Thailand and Singapore, as applicable.

The Company will generally retain its records for a period of 7 years. Records relating to ongoing investigations or transactions that have been the subject of a disclosure shall be retained beyond the stipulated retention period until it is confirmed that any investigation thereon has been closed.

The Accounting Act B.E. 2543 (2000) of Thailand its implementing documents require any corporate entity established under the laws of Thailand (including a private limited company) to maintain its accounts and relevant documents for not less than five (5) years as from the date on which each of such accounts is closed, and keep such accounts and relevant documents at its place of business. Accounts include inventory and ledger accounts. Relevant documents include copies of invoices and receipts.

IV.2.2 Reportorial Requirements

(a) Reporting of suspicious transactions

A system for the mandatory reporting and record keeping of suspicious transactions shall be instituted, including (a) the designation of the Company’s CFO as the chief reporting officer with full responsibility for the Company’s Anti-Money Laundering Program, and (b) establishing reporting units in the Company’s departments, who will be made responsible for handling the reports in respect of the respective departments and keeping such records.

Reports on suspicious transactions must be done as soon as reasonably practicable (and in any case, within ten (10) working days) after initial detection of facts that may constitute a basis for filing such reports¹¹.

Where these facts relate to potential terrorist financing or terrorist property, a report should be submitted to the relevant authorities immediately¹².

¹¹ Under section 39 of the CDSA, suspicious transactions must be reported to the Suspicious Transactions Reporting Office (STRO), a division within the Commercial Affairs Department of the Singapore Police, as soon as reasonably practicable.

¹² Under section 8 of the TSFA, a person in possession, custody or control of terrorist property or having information of any terrorist transaction must immediately inform the Commissioner of Police.

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 13 of 14

Neither the Company nor its Employees shall warn the respective third party business partner(s) when suspicious transactions are being investigated and/or information relating to them is being reported.

(b) Cross-border cash transactions

The CDSA prohibits any person from moving, or attempting to move, into or out of Singapore cash exceeding S\$20,000 in value (or its equivalent in a foreign currency) without reporting such movement to the STRO or an immigration officer (as applicable). Additionally, a person who receives cash exceeding S\$20,000 in value (or its equivalent in a foreign currency) from outside Singapore must make a report to the STRO within five business days of receipt. A person who enters or leaves Singapore carrying cash exceeding S\$20,000 in value (or its equivalent in a foreign currency) must report to an immigration officer at the Customs Red Channel when arriving in Singapore, or at the immigration counter upon departure from Singapore¹³.

For these purposes, “cash” includes any physical currency or bearer negotiable instrument (e.g. traveller’s cheques). Exceptions from this prohibition are available for certain types of person – e.g. persons who move into or out of Singapore a bill of lading, airway bill, warehouse receipt or cargo receipt¹⁴.

(c) Internal procedures

Furthermore, written internal reporting procedures are required to be implemented which shall:

- Enable all the Company's Employees to know to whom they should report any knowledge or suspicion of money laundering activity;
- Ensure that there is a clear reporting chain under which suspicions of money laundering activity will be passed to the appropriate person/unit, duly identified and designated as the reporting officer/unit;
- Require the reporting officer/unit to consider any report in the light of all relevant information available to the officer/unit for the purpose of determining whether or not it gives rise to a knowledge or suspicion of money laundering; and
- Ensure that the reporting officer/unit has/have reasonable access to any other information which may be of assistance to the officer/unit and which is available to the relevant Person.

IV.2.3 Auditing

Company personnel will conduct periodic audits of relevant Company operating units to help ensure the Company’s continued compliance with this Policy. Suspected violations will be reviewed and investigated as appropriate and may lead to disciplinary action. Any such reporting shall be treated as confidential to the extent permitted by law.

¹³ Please see Part VIA of the CDSA and the Corruption, Drug Trafficking and Other Serious Crimes (Cross Border Movements of Physical Currency and Bearer Negotiable Instruments) Regulations 2007.

¹⁴ Please see section 48B of the CDSA and the Corruption, Drug Trafficking and Other Serious Crimes (Cross Border Movements of Physical Currency and Bearer Negotiable Instruments) (Exemption) Order 2007.

Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual: AML-CTF 00		Date: 22-April-20
Title: Anti-Money Laundering and Counter-Terrorist Financing Compliance Manual	Rev: 0	Page: 14 of 14

V. Administration of the Policy

The CFO and Legal Department shall be responsible for administration, interpretation, application and periodical review of this policy. However, the decision of Managing Director or CEO will be final in the case of difference in the interpretation of any of the clauses of the policy.

Further, the Managing Director is empowered to recommend and approve any amendment in the policy, suo-moto or on the recommendation of the CFO and Legal Department.

The Company shall provide education and training for all its Employees to ensure that they are fully aware of their personal obligations and responsibilities in combating money laundering and to be familiar with its system for reporting and investigating suspicious matters.

The general scope of the training programs shall be as follows:

- New Employees – a general appreciation of this policy, the background to money laundering and the need to be able to identify suspicious transactions and report such transactions to the appropriate designated point within the Company. This training shall be provided to all new Employees, regardless of level of seniority.
- "Front-line" Employees – personnel who may be in direct contact with potential money launderers will, in addition to the training generally available to all of the Employees, be trained to identify and deal with suspicious transactions (particularly where large cash transactions are involved).
- Supervisors and Managers – a higher level of instruction covering all aspects of money laundering procedures should be provided to supervisors and managers. This will include the offences and penalties arising from applicable laws and regulations, procedures relating to service of production and restraint orders, internal reporting procedures, and the requirements for verification of identity and the retention of records.

Annual review of this AML/CTF shall be undertaken by the Legal Department. Annual refresher trainings shall be scheduled to ensure that the Employees are reminded of their responsibilities and to make them aware of any changes in the laws and rules relating to money laundering, as well as the internal procedures of the Company.