



Clean Max Enviro Energy Solutions Limited.

THIRD PARTY DUE DILIGENCE GUIDELINES

BRIBERY & CORRUPTION RISKS

May 2023

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

Versions and History

Version	Date	Summary of Changes
1.0	25 May 2023	Version 1

CONTENTS

Contents	2
Background.....	3
Key Principles	3
Applicability to Joint Ventures and Partnerships	3
Guidelines.....	3
1. Collect information about the third party and complete the Supplier Request Form. Verify and evaluate the collected information and assign an initial risk rating	4
2. Assess risk and conduct additional due diligence	4
2.1. Initial Risk rating	4
2.2. Additional Due Diligence.....	5
2.3. Assign Final Risk Rating	5
3. Negotiate contract terms in conjunction with Legal	5
4. Document and Maintain Records of Due Diligence Performed.....	6
5. Establish appropriate monitoring and risk mitigating activities	6
ANNEXURE A.....	7
Red Flags Checklist.....	7
Company Structure.....	7
Relationships with Public Officials and Governments	7
Qualifications/Experience	7
Investigations	8
Anti-Bribery and Corruption Program.....	8
Physical Location	8
Third-Party Payment Request.....	8
References	8
Other	8
ANNEXURE B.....	10
Supplier Request Form	10
ANNEXURE C.....	11
Risk Assessment Form	11
ANNEXURE D	12
Third-Party Risk Assessment.....	12
ANNEXURE E	13
Vendor Coding	13

BACKGROUND

This policy is to provide rules and guidelines to be adopted and followed by Clean Max Enviro Energy Solutions Limited, its subsidiaries and joint ventures (“**CMES**” or “**Organization**”), and their employees (to the extent as set out in this document).

As stated in our Anti-Bribery and Anti-Corruption Policy (the “**ABC Policy**”), the Organization is committed to conducting its business with honesty and integrity and in full compliance with applicable bribery or corruption laws. The ABC Policy reflects the standards to which any person or entity should adhere when acting on the Organization’s behalf, including partners, agents and contractors.

Third parties are not permitted to pay, offer, accept or request bribes on behalf of the Organization. While working with third parties is a necessary part of the business, the Organization needs to be mindful that it may be prosecuted for failing to prevent bribery by a third party acting on its behalf.

To support this commitment, the Organization requires that appropriate due diligence be conducted with respect to its third parties. Effective due diligence can mitigate third party liability issues and help manage associated reputational and financial risks.

The Organization’s Anti-Bribery, Anti-Corruption and Anti-Money Laundering Program (the “**ABC Program**”) provides additional information on our approach to help prevent and detect bribery as part of our overall internal control framework.

These guidelines provide additional information on the due diligence and bribery risk assessment process when assessing third parties.

Implementation of this Policy will be undertaken within the timelines and in the manner as stipulated under the ABC Program.

KEY PRINCIPLES

The Organization transacts and does business with a variety of third parties: vendors, consultants, partners, joint venturers, and service providers.

Third parties will be assessed for bribery and corruption risk and assigned a risk category ranking of “High”, “Medium”, or “Low”. In some situations, business judgment will be required in assigning the risk category. Risk mitigating procedures and monitoring activities should be established for each of the risk categories as appropriate.

Throughout the relationship with the third-party, attention should be given to potential red flags that may arise. Red flags are activities that increase the likelihood of a potential violation of the ABC Policy or relevant bribery and corruption laws. Red flags are not meant to stop the business from operating but indicate that caution and additional scrutiny may be required. These red flags often occur outside the normal contracting and initial transaction process. Refer to ANNEXURE A for examples of red flags.

APPLICABILITY TO JOINT VENTURES AND PARTNERSHIPS

The Organization may also be liable for the actions of joint venturers or partners, as they may be seen as acting on the Organization’s behalf in certain circumstances. In addition, a joint venture or partner could cause one of our joint ventures or partnerships to engage in bribery or corruption, which might create issues for the joint

venture, partnership, and/or the Organization. Consequently, these due diligence procedures also apply to joint venturers and partners.

GUIDELINES

The process for assessing and managing the bribery and corruption risks associated with third parties consist of the following steps:

1. Collect information about the third party and complete the Supplier Request Form. Verify and evaluate the collected information.
2. Assess risk and conduct additional anti-bribery and anti-corruption due diligence as appropriate.
3. Negotiate contract terms in conjunction with Legal (if applicable)
4. Document and maintain records of the due diligence performed.
5. Establish appropriate monitoring and risk mitigating activities.

The extent of due diligence conducted should be based on the evaluation of bribery and corruption risk (i.e., higher degree of bribery and corruption risk requires more extensive due diligence). The specific methods for due diligence will vary depending on the bribery and corruption risks identified. Where risk assessments and additional due diligence are required, supporting documentation should be maintained to substantiate the due diligence conducted and the conclusions reached.

The Organization should ensure that third parties acting on its behalf understand the ABC Policy and agree to act consistently with its principles. Where appropriate, third parties should provide certifications confirming their understanding and adherence to the ABC Policy. Other contractual provisions and risk mitigation plans, including ongoing monitoring, may also be appropriate, depending on the third party's risk category.

STEPS:

1. COLLECT INFORMATION ABOUT THE THIRD PARTY AND COMPLETE THE SUPPLIER REQUEST FORM. VERIFY AND EVALUATE THE COLLECTED INFORMATION AND ASSIGN AN INITIAL RISK RATING

Know your potential third party and make appropriate enquiries.

Information Gathering

For all vendors, complete the Supplier Request Form. See ANNEXURE B.

Information gathered through the Supplier Request Form will assist in determining the level of additional due diligence to be performed. Certain sections of the Supplier Request Form will need to be completed and signed by a representative of the third party.

Prior to engaging with the third party, consider the associated level of bribery and corruption risk, such as:

- The need and business justification to retain the third party
- The residence and operating location, industry, and affiliation of the third party (refer to Transparency International for the country risk index)
- The business reputation and qualifications
- The beneficial owners/principals (i.e., are any of them public officials?)
- The proposed activities and whether the third party will be dealing with government officials or entities (e.g., for permits, licenses, approvals, taxes, lobbying)
- The amount and terms of compensation (i.e., a large success fee would be a red flag)
- Whether the third party will be "acting on our behalf" (e.g., acting as an agent or otherwise representing the Organization in dealings with outside parties)
- Procurement of goods and services in high bribery risk countries or industries
- The results of background checks, media, and litigation searches (e.g., Dow Jones diligence)

- Consider any red flags identified in the verification process and determine whether they can be adequately addressed.

2. ASSESS RISK AND CONDUCT ADDITIONAL DUE DILIGENCE

The degree of due diligence should be commensurate with the assessed level of bribery and corruption risk.

2.1. INITIAL RISK RATING

Based on the information gathered, the degree of bribery or corruption risk should be assessed, and an initial risk rating should be assigned (High, Medium, or Low and in the case of employees XLow). A Risk Assessment Form which provides additional risk indicators to consider, may be completed in order to assist with establishing the initial risk rating (See **ANNEXURE C**).

2.2. ADDITIONAL DUE DILIGENCE

No additional due diligence is required where an initial rating of Low Risk is assigned. However, the inclusion of certain anti-bribery provisions in the contractual agreement should be considered.

Additional due diligence is required where an initial rating of Medium Risk or High Risk is assigned. See ANNEXURE D for additional guidance on performing additional diligence.

2.3. ASSIGN FINAL RISK RATING

Based on the information obtained, assign and document the Final Risk Rating and determine whether the third party should be approved. Record the Final Risk Rating in the “Risk” field of the vendor profile in the ERP system (if available).

Note: the assignment of Final Risk Rating for an initial Medium or High Risk third party and the approval of the third party should be conducted by an individual independent from those proposing to engage the third party.

If the third party is approved, negotiate appropriate contract terms and develop other risk mitigation plans as applicable.

3. NEGOTIATE CONTRACT TERMS IN CONJUNCTION WITH LEGAL

Based on the results from previous steps, negotiate appropriate contract terms with the third party

Consult with Legal as to the form of the agreement or the contract that maybe required, especially if the third party is acting on behalf of the Organization. Depending on the services or work to be performed, the agreement or contract may include provisions such as:

- Description of goods/services to be provided
- Description of pricing/compensation, payment terms (e.g., billings supported by invoices detailing goods/services provided), and expense reimbursement arrangements (e.g., reimbursement for actual expenses supported by invoices is better than a per diem)
- Procedures for use of subcontractors/agents (e.g., prior approval) and limiting the third party’s ability to act on the Organization’s behalf and/or to interact with government officials/entities
- Prohibition on all types of bribery and corruption
- Representation that the third party has appropriate ABC policies and procedures, and anti-bribery representations/undertakings/warranties and regular (e.g., annual) certifications of compliance
- Require the third party to comply with the Organization’s ABC Policy and applicable anti-bribery and anti-corruption laws

- Require the third party to maintain accurate books and records, and in some circumstances, require the third party to grant the right to audit the third party's books and records on a regular basis or if an incident arises
- Requirement to notify the Organization of breaches of the agreement and of pending or initiated bribery-related investigations
- Right to terminate contract for and indemnification from breach of terms, as applicable
- Right to demand information related to possible bribery and corruption incidents

Also, be aware of red flags that may arise during negotiations, and therefore require an update to due diligence and risk assessment.

4. DOCUMENT AND MAINTAIN RECORDS OF DUE DILIGENCE PERFORMED

Be able to show that appropriate due diligence was performed for each third-party

Appropriate records should be maintained (i.e., as part of the vendor record in the ERP application or other central location) including the information obtained from the third party or from additional sources used in assessing third party risk. The list of approved vendors should be maintained in the ERP application as part of the vendor master file.

5. ESTABLISH APPROPRIATE MONITORING AND RISK MITIGATING ACTIVITIES

Establish the process for identifying changes in the third-party risk ranking.

Each operating business within the Organisation (**Operating Business**) is responsible for mitigating the risk and monitoring of third parties to identify factors impacting the risk rating.

Where a third party has previously been engaged and assessed for bribery and corruption risk, additional due diligence is not necessary unless the third party has been categorized as High Risk or its risk ranking increases based on the nature of the engagement (e.g., the third party is asked to conduct work in a riskier region).

When engaging the third party that was assessed as High Risk, consider the following risk mitigating activities:

- Include additional ABC provisions in the contract or agreement that are appropriate for the risk rating of the third party.
- Provide training to the third party on the ABC Policy.
- Identify a member of senior management to review and approve invoices for payment.

Due diligence on High Risk third parties should be updated at least annually, or sooner if circumstances warrant. For Medium and Low Risk third parties, the due diligence should be updated at least every three and five years, respectively. Operating Businesses can consider using a risk database (such as Dow Jones) for continuous monitoring of high and/or medium risk third parties.

Periodically, the Operating Business should review the list of vendors and identify those that should be deactivated from the approved vendor listing in the ERP application or the approved vendor list. The assessment should consider the time passed since the last transaction, open purchase orders, requirement for ongoing relationship, etc.

ANNEXURE A

RED FLAGS CHECKLIST

A “**Red Flag**” is an activity or a condition that increases the likelihood of a potential violation of the ABC Policy or of the anti-bribery and corruption laws. Red flags are not meant to stop the business from operating, but to indicate that caution and additional scrutiny may be required.

If red flags have been identified, further inquiries, including seeking advice from a senior executive, Internal Legal Counsel or the Financial Controller of the Organization, may be required.

Red flags may be uncovered in responses to the Supplier Request Form and/or in verifying the information obtained from the third party. Not all red flags suggest that an issue exists or that the Organization cannot engage the third party. However, the appearance of a red flag generally requires more in-depth review. Explanations of the inquiries made, and supporting documentation, should be maintained to substantiate the due diligence conducted and the conclusions reached.

Examples of red flags in dealing with third parties include, but are not limited to the following:

Company Structure

- Refusal to provide details of ownership, partners or principals or to cooperate in the diligence process.
- Third party operates in a high-risk country or industry per the Transparency International Country Perception index.
- Third party is incorporated in an offshore jurisdiction.
- An officer, senior executive or key employee of the third party has an interest in or is related to an officer, senior executive or key employee in another company that might be considered a competitor to the third party.
- Third party appears to be a shell company or has some other unorthodox corporate structure.

Relationships with Public Officials and Governments

- Third party is directly or indirectly owned in whole or in part by a government entity, a public official or political party.
- Third party has been championed (directed) by a public official or representative to be part of the transaction.
- Third party principal has a relative or close family relation (e.g., spouse, in-law, sibling, parent) who has been or is regularly involved with public officials, local or national politicians, potential competitors, political activists, or others in a position to influence business decisions.
- Third party employs personnel who are current or former public officials for the services being carried out for CMES.
- Third party or affiliated entities appear on state-owned entities (SOE) databases and have not been disclosed.
- A principal, owner, senior executive or key employee of the third party is on a watch-list and/or politically exposed persons (PEP) database.
- Third party uses consultants/agents to win or retain public sector business, assist in contract tenders with government customers (e.g., lobbyists) or obtain licenses.

Qualifications/Experience

- Third party does not demonstrate industry experience with products or service, or is in a different line of business than for which it has been engaged.
- Third party appears on a list of those debarred from bidding on local, national or international contracts (e.g., World Bank Listing of Ineligible Firms & Individuals)

- Records from the official registry of companies do not agree with the information provided by the third-party regarding ownership, directorships or other details.
- Qualifications claimed by the third party are denied by the issuing body.
- Third Party lacks customarily associated staff and facilities.

Investigations

- Third party, including its principals or other employees, has been or is currently suspended or otherwise censored in business dealings or criminally charged with or prosecuted for alleged fraud, bribery, misrepresentation and/or any other criminal act.
- Third party or any of its principals have a reputation for, or have been accused of, corruption or improper business practices (e.g., in the media and otherwise) or it would be embarrassing to the third party or CMES were its practices to be publicly reported.
- An official body advises of a criminal conviction that has not been disclosed by third party.
- Third party has a pattern of frequent and continued involvement in litigation.

Anti-Bribery and Corruption Program

- Third party has not established any internal policies prohibiting corruption or bribery and refuses to put such measures in place.
- Third party declines to complete basic intake questionnaire.
- Third party makes large or frequent political contributions.
- Third party has inadequate policies and controls on gifts and other expenses.

Physical Location

- Third party offices are in an unusual area or are otherwise significantly different from similar businesses (e.g., in highly industrial areas, in residential areas, where the company's name is not indicated, have significant levels of security or highly restricted).
- Electoral or local business records show a different location for the third party.
- Third party is located in a country other than where its services are being performed.

Third-Party Payment Request

- That payment be made to an offshore bank account.
- That payment be made through another company or individual.
- Terms of the contract indicate payment by cash, substantial up-front or advance payments not customary for the industry, or excessive success fees.

REFERENCES

- Third party offers references who are evasive, uncooperative or not forthcoming.
- There are significant variances between the information provided by the third party and the information provided by the references.

OTHER

- Third party makes suspicious statements such as needing money to "get the business" or "make the necessary arrangements".
- Third party initiates things that suggest a proclivity for or familiarity with corrupt activity and how to manage or manipulate people, systems or safeguards in order to get a desired business outcome.
- Third party proposes hiring an affiliate whose skill set and mandate are redundant or whose resume and/or history does not appear suited to the job at hand.

- Third party seeks to perform services without a written agreement or refuses to agree to anti-bribery/corruption provisions/certifications.
- Third party has inadequate or no books and records.
- Information/responses received from third party are incomplete, inconsistent or misrepresented.
- Third party make requests for political or charitable contributions.

ANNEXURE B

Supplier Request Form

The Supplier Request Form captures the relevant information required to onboard a vendor or third party, including information required to perform an initial assessment of third-party ABC risk. It is important to also code vendors by type and record this information in the ERP application, if applicable (see **ANNEXURE E**).

The Supplier Request Form must, at a minimum, include the following anti- bribery related questions:

- Location where the work/services will be performed.
- Has the third party or any of its principals, owners, directors/officers, senior management, or employees ever been the subject of an ABC allegation or investigation or been convicted of a crime?
- Is the beneficial ownership of the third party held wholly or partly by a government official/ entity or a public official?
- Are owners, directors/officers, senior management, affiliated with government officials/ entities?
- Will the work/services to be performed require interaction with government officials/entities?
- Will the third party engage a further third party to conduct work on BEP's behalf?
- the third party involved in any joint ventures and/or lobbying with government or quasi- government officials/entities?
- Does the third party have a written ABC policy in place covering compliance with anti-bribery and corruption laws?

The Supplier Request Form must be signed by the requestor and be approved by the Procurement department.

ANNEXURE C

Risk Assessment Form

The Risk Assessment Form allows for an initial assessment of third-party ABC risk to be performed.

The Risk Assessment Form, must, at a minimum, assess the level of ABC risk in the following areas:

- Location of the third-party (operations, principal office, where work/services will be performed)
- Supplier type (as per ANNEXURE E)
- Background of the third-party (as per due diligence research, investigations/convictions/history of ABC allegations, existence of written ABC Policy)
- Government and political affiliations
- Scope of work acting on behalf of CMES

When any area of the Risk Assessment Form receives an initial risk rating other than Low, the Form must be escalated as per the process in each Operating Business (i.e., to Legal or Compliance).

ANNEXURE D

Third-Party Risk Assessment

Third parties will be assigned a risk category ranking of “High”, “Medium” and “Low” and this ranking will be recorded in the “Risk” field of the vendor record in the ERP application or any other central location. Employees will be assigned a risk category ranking of XLow and will not be required to complete a Supplier Request Form.

Business judgment will be required in the recording of the third-party risk category. Typically, approximately 5% of the third parties would be High Risk, 15% Medium Risk and 80% Low Risk.

Note: The Organization operates in a highly regulated environment and, as part of our normal course of business, employees are expected to have interactions with government officials/entities. The Organization is also required to pay government entities for licenses and permits (with recurring and transparent fee schedules) to operate power generating assets. Thus, while such government entities are not typically considered High Risk, the appropriate degree of diligence should still be completed.

For Medium Risk third parties, additional due diligence to consider, if applicable, includes:

- Conducting online research in risk and compliance databases (i.e., Dow Jones) and international media, to identify risk-relevant information regarding the third party and/or its owner(s)/principal(s)
- Search global intelligence databases (e.g., Lexis Nexis, World Bank) covering government-prohibited persons/entities, politically exposed persons (“PEPs”), and persons/entities linked to corruption.
- Obtain online “Business Information Report” from Dun & Bradstreet or equivalent resource to confirm corporate history and stability and to uncover any potential adverse media coverage.
- Conduct a Google search for key words and terms.

For High Risk third parties, additional due diligence to consider, if applicable, includes:

- The additional due diligence for Medium Risk third parties above.
- Examine detailed business profile (e.g., who are the third party’s other clients/contacts), request and review the third party’s Code of Conduct, relevant internal policies, and bank references (seek assistance from the Legal or Risk Groups as needed).
- Review corporate records from business registries to identify shareholders, directors/officers, and other affiliated individuals.
- Search relevant public local criminal records/law enforcement databases.
- Search court records, to identify information indicating involvement in criminal/civil litigation, bankruptcy, or other disputes.
- Search regulatory records to identify adverse/disciplinary actions taken by local and/or central regulators.
- Meeting with third party management

ANNEXURE E

VENDOR CODING

Third parties should be classified and coded in the ERP system or the approved vendor list. The following categories should be used:

1. Government entity or public official
2. Lobbyist
3. Joint venture partner
4. Consultant/Service Provider
5. Construction Contractor
6. Goods/Parts Provider
7. Donation
8. Related Party to BEP
9. Landowners (i.e., for wind/ solar farms that are operated by CMES)
10. Employee
11. Intercompany

Operating Businesses may consider adding more vendor categories such as the following:

1. Customs agent or broker providing customs clearance.
2. Legal
3. Permit or Licensing agency