CanadianSolar

Apr 10, 2026

WHISTLEBLOWER POLICY

Whistleblower Policy and Procedures (the "*Policy*") of CSI Solar Co., Ltd. and its Subsidiary Entities

Table of Contents

This is the English translation of Chinese version, in case of any discrepancy, the Chinese version shall prevail.

INTRODUCTION

CSI Solar Co., Ltd. ("***CSI Solar***") is committed to maintaining the highest standards of conduct and ethics in the way that it conducts its business. The Code of Business Conduct and Ethics (the "***Code***") of CSI Solar and its subsidiary entities (the "***Company***") describes the standard of conduct and ethics which should be complied with by all directors, officers and employees (together, the "***Employees***") of the Company.

INTENT OF POLICY

The Code requires all Employees to report Concerns with respect to violations of the Code (the "***Concerns***"), including incidents of retaliation against Employees who report Concerns in good faith. It is in the interests of all stakeholders of the Company that all Concerns be reported so that they can be properly addressed.

This Policy is a supplement to the Code and is intended as a control method to help safeguard the integrity of the Company's financial reporting and business dealings by supporting adherence to the Code, including the reporting of Concerns, protecting Employees who report Concerns in good faith and setting out procedures for the receipt, retention and treatment of documents relating to reported Concerns.

POLICY

Types of Concerns to be Reported

All Employees have a responsibility to report Concerns, including Concerns reported by external parties such as customers and suppliers, and to cooperate with the investigation of reported Concerns.

This Policy deals with Concerns related to the following illegal or non-compliant activities:

Breaches in Financial Reporting and Disclosure – including but not limited to financial reporting fraud (e.g., manipulation of financial statements, overstatement of revenue, concealment of liabilities or expenses) and falsification of business data (e.g., misreporting of sales data, production data, or KPI indicators).

Misappropriation of Assets and Expense Fraud – including but not limited to misappropriation of assets (e.g., theft of the Company's cash, inventory or equipment, misuse of company funds, or use of Company assets for personal purposes) and expense fraud (e.g., false claims for travel, business courtesy or procurement expenses, or fabrication of supporting documents to improperly obtain funds).

Unauthorized Leakage of Confidential Information – including but not limited to the unauthorized leakage of the Company's trade secrets such as technical secrets, customer lists, procurement prices, and strategic plans, or the unauthorized leakage of other internal information that has not been publicly disclosed but has a material impact on the Company's operations, business decisions, or legitimate interests, as well as acts of malicious system sabotage, unauthorized access, or access beyond authorized privileges.

Improper Business Conduct – including but not limited to holding equity interests in or operating businesses that compete with the Company, or improperly diverting the Company's business opportunities for personal gain.

Environmental, Health, Safety and Social Responsibility Violations – including but not limited to concealing safety production incidents or occupational health events that are required to be reported.

Bribery and Corruption – including but not limited to conflicts of interest (e.g., where an employee or his/her relatives hold interests in external entities having business dealings with the Company and the employee uses his/her position or authority to obtain improper benefits for himself/herself), bribery and kickbacks (e.g., accepting or soliciting kickbacks, gifts or other improper benefits from suppliers or customers, or offering bribes to government officials or other external parties), as well as nepotism (e.g., improper recruitment or promotion of relatives).

Employee Rights and Workplace Conduct Violations – including but not limited to workplace sexual harassment, retaliation against employees who report concerns, and improper collection or use of personal privacy information.

Other Violations of Laws, Regulations or the Company's Compliance Policies/Management Procedures – violations of other applicable laws, regulations or the Company's compliance policies/management procedures, other than the illegal or non-compliant activities described above.

Violations of the Company's Policies/Management Procedures or Control Processes – conduct that does not constitute the above-mentioned fraud or illegal or non-compliant activities, but clearly violates the Company's key policies/management procedures or control processes (e.g., violations of policies, management procedures or control processes relating to procurement, expense reimbursement, information security, recruitment or promotion).

Reporting Channels

There are several channels through which Employees may report Concerns. Consideration should be given to the nature of the Concern in choosing the most appropriate channel.

	Channel	Contact Details
1.	Chain of Communication	The Company has well-established procedures to enable Employees to escalate Concerns through the normal chain of communication (i.e., their supervisors and members of the Human Resources Department). This should be the channel of choice for most Concerns, particularly those relating to Human Resources matters
2.	Contact the Compliance Officer	Byron Xu +86 512 689 65711 byron.xu@csisolar.com
3.	Contact the Head of Corporate Internal Audit	Tina Bai +86 512 689 66642 tina.bai@csisolar.com
4.	Call the Whistleblower Hotline	Worldwide: +1 519 823 7451 China: +86 512 689 66888
5.	Write to the Whistleblower Email	whistle-blower@csisolar.com

The Company will treat all reported Concerns seriously and deal with them expeditiously.

All Concerns may be reported on an anonymous basis. If a Concern is reported anonymously, the identity of the individual reporting the Concern (the "***Claimant***") will not be known to the Company. ***Important Note***: Reporting anonymously can limit the ability of the Company to thoroughly investigate a reported Concern if insufficient information is provided.

The Company's customers, suppliers and business partners and other external parties may also report Concerns.

Concerns reported through the Whistleblower Hotline are automatically directed to the Compliance Officer and the Head of Corporate Internal Audit (the "***Primary Recipient***").

All significant Concerns, including significant Concerns reported by external parties, will be provided to the Board or President by the Primary Recipient, as appropriate, depending on the nature of the Concern, to ensure independent review, investigation and disposition.

Investigation

Upon receipt of a significant Concern, the Primary Recipient will evaluate the severity of the Concern to determine whether an internal or external investigation is required.

The Primary Recipient will then assign the investigation accordingly to the relevant person/department and maintain oversight of the investigation to ensure appropriate and timely resolution.

Reporting

To the Board or President – The results of investigations of all significant Concerns will be reported to the Board or President quarterly or more frequently if necessary.

To Executive Management – The results of investigations of all Concerns will be reported to the appropriate senior officers of CSI Solar ("***Executive Management***") in order to advise them of the disposition and/or to ensure proper resolution of the Concerns.

To the Claimant – The results of investigations of Concerns may be reported to the Claimant where possible.

Protection from Retaliation

In investigating Concerns, the Company will protect the confidentiality and anonymity of the Claimant to the fullest extent possible, consistent with the need to conduct an adequate review of the Concerns. ***Important Note***: The Company is not obligated to protect the confidentiality and anonymity of external parties (i.e., non-Employees) who report Concerns.

The Company will protect from retaliation any Employee who reports a Concern in good faith in accordance with the methods described in the Code or this Policy. Retaliation against the Employee will not be tolerated. An Employee who retaliates against someone who has reported a violation in good faith is subject to disciplinary action which could include termination of employment.

Retention of Records

The Company will retain all documents relating to Concerns reported to the Company for at least five years from the date that the Concern was reported, after which the documents may be destroyed unless the documents may be relevant to any pending or potential litigation, inquiry or investigation, in which case the documents may not be destroyed and will be retained for the duration of the litigation, inquiry or investigation and thereafter as necessary.

ROLES AND RESPONSIBILITIES

The Board

The role and responsibility of the Board:

- Determining the appointment or dismissal of the Head of Compliance.
- Authorizing the Head of Compliance to accept and hear the Concerns within his/her scope of duties, organize or participate in the investigation of violations and propose the disciplinary action.

- Determining the disciplinary action of the violator in accordance with the authority.

President

The role and responsibility of the President:

- Approving this Policy.
- Taking measures to ensure the effective implementation of this Policy.
- Prohibiting and correcting the non-compliant business activities, investigating the violator's responsibility and proposing the disciplinary action in accordance with the authority.

Compliance Officer and/or Head of Corporate Internal Audit

The role and responsibilities of the Compliance Officer and/or the Head of Corporate Internal Audit are as follows:

- Developing and maintaining this Policy.
- Overseeing the operation and maintenance of the Whistleblower Hotline.
- Receiving, investigating and taking action with respect to significant Concerns.
- As appropriate, referring Concerns to Human Resources Department or other relevant departments for handling.
- Communicating with Employees who have raised Concerns.
- Reporting to the Board or President and Executive Management.
- Consolidating, filing and retaining records of all Concerns received together with the status and results of their investigation.

Human Resources Department

The role and responsibilities of Human Resources Department are as follows:

- Consulting on the development and maintenance of this Policy.
- Communicating the Code and this Policy to Employees.
- Conducting or assisting in the investigation of human resources related Concerns and reporting the results to the Compliance Officer and/or the Head of Corporate Internal Audit.

Business Departments and Executive Management

The role and responsibilities of the Business Departments and Executive Management are as follows:

- Communicating and enforcing the Code and this Policy.

- Conducting or assisting in the investigation of Concerns reported through the chain of communication or by external parties and/or directing such Concerns to the Compliance Officer and/or the Head of Corporate Internal Audit for investigation as appropriate.

All Employees

The role and responsibilities of all Employees are as follows:

- Complying with the Code and this Policy.
- Assisting with the investigation of Concerns when required.

ANNEX 1

SPECIFIC RULES APPLY TO EMEA WHISTLEBLOWER

INTRODUCTION

The EU General Data Protection Regulation ("***GDPR***") limits and protects the transfer of personal data outside the European Economic Area ("***EEA***"). Recent Directives of the European Union on the protection of whistleblowers also require the adoption of common minimum standards within the European Union, to ensure balanced and effective whistleblower protections.

It is in the interests of all stakeholders of the Company to comply with all applicable legislation on data protection and on the protection of whistleblowers that report violations of the Company's policies.

This Appendix I is a supplement to the Policy to be applied to whistleblowing and reporting procedures connected exclusively to EMEA's activities. It is intended to protect EMEA's Employees who report Concerns in good faith and set out procedures for the receipt, retention, and treatment of documents and/or electronic files relating to reported Concerns.

POLICY

EMEA's Reporting Channels

There are several channels through which EMEA's Employees may report Concerns. Consideration should be given to the nature of the Concern in choosing the most appropriate channel.

	Channel	Contact Details
1.	Chain of Communication	The Company has well-established procedures to enable Employees to escalate Concerns through the normal chain of communication (i.e., their supervisors and members of the Human Resources Department). This should be the channel of choice for most Concerns, particularly those relating to Human Resources matters
2.	Contact EMEA's Compliance Manager	Carlos Coutinho carlos.coutinho@csisolar.com

	Channel	Contact Details
3.	Report an Incident on the internet	Via the following link https://app.convercent.com/en-US/LandingPageView/ReportIssue/8aabe6d6-ea7a-ec11-a989-000d3ab9f062
4.	Call EMEA's Whistleblower Hotline	Germany: 0800.181.2396 Spain: 900.905460 South Africa: +27-105004106 Other locations: visit speakupcsisolar.com

The Company will treat all reported Concerns seriously and deal with them expeditiously.

All Concerns may be reported on an anonymous basis. If a Concern is reported anonymously, the identity of the Claimant will not be known to the Company. ***Important Note***: Reporting anonymously can limit the ability of the Company to thoroughly investigate a reported Concern if insufficient information is provided.

The Company's customers, suppliers and business partners and other external parties may also report Concerns.

Concerns reported through the Whistleblower Hotline are automatically directed to EMEA's Compliance Manager (the "***EMEA's Primary Recipient***"), and all data is recorded and kept within the borders of EEA.

All significant Concerns, including significant Concerns reported by external parties, will be provided to Compliance Officer by EMEA's Primary Recipient, to ensure independent review, investigation and disposition.

Retention of Records

The Company will retain all documents and electronic files relating to Concerns reported to EMEA, at network and information systems within the borders of the EEA. Such records will be retained for at least five years from the date that the Concern was reported, after which the documents and/or electronic files may be destroyed unless the documents and/or electronic files become relevant to any pending or potential litigation, inquiry or investigation, in which case the documents and/or electronic files may not be destroyed and will be retained for the duration of the litigation, inquiry or investigation and thereafter as necessary.