Certified Emissions Reduction Technologies Foundation

WHISTLEBLOWER POLICY

Protected Reporting, Investigation and Anti-Retaliation Framework

Document ID: CERT-GOV-004
Version 1.0 (Draft for Consultation)
Date: 2 July 2026
Classification: Public

Document Control

Field	Detail
Document ID	CERT-GOV-004
Title	CERT Whistleblower Policy
Version	1.0 (Draft for Consultation)
Status	Draft – pending Board adoption and public consultation
Owner	Ethics and Integrity Committee
Approver	Board of Trustees
Review cycle	At least every three years, or upon material change
Related documents	CERT-FDN-001 (Clause 14); CERT-GOV-002; CERT-GOV-003; CERT-GOV-005; CERT-REG-007 (planned)

Version History

Version	Date	Author	Description
1.0	2026-07-02	CERT Founding Secretariat	Initial draft for founding Board review and public consultation.

Table of Contents

1. Purpose and Scope

1.1 CERT's credibility depends on people being able to raise integrity concerns safely — including concerns about CERT itself. This Policy implements Charter Clause 14.1 by establishing protected reporting channels, investigation procedures, and anti-retaliation guarantees.

1.2 Who may report. Anyone: CERT Persons (as defined in the Code of Ethics), employees of project proponents, VVBs, market participants, community members affected by projects, and members of the public. Protection under this Policy does not depend on employment by CERT.

1.3 Indian law interface. CERT is incorporated in India. Where CERT is constituted as a Section 8 company to which the vigil-mechanism requirements of Section 177(9) of the Companies Act, 2013 and Rule 7 of the Companies (Meetings of Board and its Powers) Rules, 2014 apply, this Policy constitutes CERT's vigil mechanism, and the Ethics and Integrity Committee performs the oversight role assigned to the audit committee thereunder. The General Counsel maintains a compliance annex mapping this Policy to applicable Indian law and to statutory regimes of other jurisdictions where CERT engages workers.

2. Reportable Conduct

Reports may concern any suspected wrongdoing related to CERT's remit, including:

- Fraud, misstatement, or manipulation in project documentation, monitoring data, validation, or verification.
- Over-crediting, baseline manipulation, or concealment of non-additionality or reversals.
- Bribery, corruption, or undisclosed conflicts of interest involving any CERT Person, proponent, or VVB.
- Double counting, double claiming, or registry record manipulation.
- Violation of environmental or social safeguards, including community rights and free, prior, and informed consent.
- Breach of CERT governance policies, information security incidents, or misuse of registry data.
- Retaliation against any reporter.

2.1 Ordinary commercial disputes and appeals against CERT decisions follow the Appeals procedures (CERT-REG-007, planned); the Secretariat shall route misdirected reports without prejudice to the reporter.

3. Reporting Channels

3.1 CERT maintains: (a) a secure web portal and hotline operated by an independent external provider, available 24/7, in the major languages of CERT's project regions, permitting anonymous reporting with two-way anonymous dialogue; (b) direct reporting to the Ethics and Integrity Committee chair; and (c) internal reporting to line management for staff, which must be logged into the central case system within two working days.

3.2 Reports concerning the Chief Executive, a trustee, or an Ethics and Integrity Committee member are handled exclusively by the Committee (excluding any implicated member), reporting to the Board Chair or, if implicated, to the full non-conflicted Board.

4. Confidentiality and Anonymity

4.1 The identity of a reporter, and information from which it could be deduced, is disclosed only to those strictly necessary for the investigation, and never to any person implicated, except where required by law with advance notice to the reporter where lawful.

4.2 Anonymous reports are accepted and investigated to the extent the information allows. Reporters are encouraged (not required) to identify themselves to enable follow-up.

5. Protection Against Retaliation

5.1 Retaliation — any detriment imposed because of a good-faith report or cooperation with an investigation, including dismissal, demotion, contract termination, blacklisting from CERT processes, harassment, or threats — is prohibited and is itself a sanctionable breach.

5.2 Where the reporter is external (e.g., a VVB employee or community member), CERT protects them by: refusing to disclose identity; treating retaliation by a CERT participant or VVB as a Rulebook integrity breach subject to sanction; and, where appropriate, referring matters to authorities.

5.3 Good faith standard. Protection applies to reports made with reasonable belief in their truth, even if unsubstantiated. Knowingly false reports are a breach of the Code of Ethics.

5.4 Burden. In any internal proceeding, once a reporter shows a report and subsequent detriment, the burden shifts to the alleged retaliator to show the detriment was unrelated.

6. Investigation Procedure

6.1 Acknowledgement within seven days. Initial triage by the case manager (independent provider or Committee delegate) within fourteen days: dismissal with reasons, referral to the correct procedure, or opening of an investigation.

6.2 Investigations are conducted under Ethics and Integrity Committee oversight by investigators with no conflict, with power to access records and interview personnel (GOV-001 §6.3). Persons implicated receive due process: notice of substance (protecting the reporter), opportunity to respond, and representation.

6.3 Target timeline: conclusion within ninety days, extendable with reasons communicated to the reporter. The reporter receives feedback on outcome to the extent lawful.

6.4 Outcomes may include: sanctions under GOV-002/GOV-003; Rulebook enforcement against participants or VVBs (suspension, credit freeze, de-accreditation); correction of registry records; referral to law enforcement or regulators; and systemic recommendations.

6.5 Interim measures. Where credible allegations concern live issuance, the Secretariat may freeze affected issuances or credits pending investigation, per the Rulebook.

7. Records, Reporting and Review

7.1 All cases are logged in a secure case-management system with access restricted to the case team; records are retained for ten years.

7.2 The annual integrity report publishes case statistics (volume, categories, outcomes, time-to-resolution) in anonymised form.

7.3 This Policy is owned by the Ethics and Integrity Committee and reviewed at least every three years, and after any case revealing a procedural weakness.