

WHISTLE BLOWER POLICY / VIGIL MECHANISM POLICY

Document Control

Version History

Version	Remarks	Date
1.0	Adopted based on Approval by Audit Committee	26 Aug 2026

BiofuelCircle Whistleblower Policy / Vigil Mechanism

1. Purpose

BiofuelCircle Private Limited is committed to lawful, ethical and responsible conduct. This Policy gives eligible persons a safe way to report genuine concerns. It also establishes the Company's statutory vigil mechanism.

The mechanism supports early detection, fair investigation, corrective action, protection against victimisation, and Board oversight. It does not replace normal management responsibility or other statutory complaint mechanisms.

2. Scope and applicability

This Policy applies to BiofuelCircle Private Limited. Each controlled subsidiary shall adopt this Policy by its governing body or adopt a local policy that meets these minimum standards. A joint venture shall be covered after adoption by its governing body or as required by its constitutional documents and applicable law.

The statutory right under Rule 7 of the Companies (Meetings of Board and its Powers) Rules, 2014 applies to directors and employees. As a governance measure, the Company also accepts reports from former employees, applicants, interns, trainees, contract workers, consultants, agents, vendors, suppliers, service providers, customers, lenders, community representatives and other business partners.

3. Guiding principles

In framing and acting under this Policy, BiofuelCircle shall

- Report genuine concerns promptly.
- Protect the Whistleblower and persons who assist an investigation.
- Restrict information to persons with a legitimate need to know.
- Use independent and conflict-free decision-makers.
- Treat the Subject fairly.
- Base findings on available evidence and the balance of probabilities.
- Preserve evidence and maintain an audit trail.
- Take corrective and preventive action.
- Not obstruct lawful reporting to a regulator, law-enforcement agency or court.

4. Definitions

Term	Meaning
Audit Committee	The Audit Committee of the Company, if constituted and authorised to oversee the vigil mechanism.
Board	The Board of Directors of the relevant Company or covered group entity.

Term	Meaning
Concern	Information that indicates possible Reportable Conduct.
Ethics and Vigilance Officer or EVO	The officer appointed to administer this Policy. The EVO is not the final decision-maker in a case involving the EVO or a conflict.
Good faith	An honest and reasonable belief that the information may show Reportable Conduct. The Whistleblower need not prove the allegation.
Investigator	An internal or external person appointed to conduct fact-finding.
Material Case	A case that meets an escalation trigger in section 17 or the case-classification matrix.
Oversight Authority	Audit Committee, if constituted; otherwise, a nominated Director under Rule 7
Policy Owner	The EVO is the owner of this Policy.
Protected Disclosure	A Concern reported under this Policy in good faith.
Reportable Conduct	Conduct listed in section 6. Matters covered
Retaliation	Any detrimental action or threat linked to a Protected Disclosure, participation in an investigation, or refusal to participate in wrongdoing.
Subject	A person or entity whose conduct is under review.
Whistleblower	A person who makes or attempts to make a Protected Disclosure.

5. Who can raise a Concern

Any eligible person may raise a Concern. A person may report conduct affecting the Company, a covered group entity, its workforce, assets, records, customers, business partners, communities or legal obligations.

A Whistleblower may report a Concern even if they are not directly affected. Managers who receive information that may indicate Reportable Conduct shall forward it promptly to the EVO. They shall not investigate it informally.

6. Matters covered

The following matters shall be considered under this Policy

- Fraud, embezzlement, theft, misappropriation or diversion of funds or assets.
- False invoices, false expense claims, fictitious transactions, improper revenue or cost recognition, or manipulation of accounts.
- Forgery, falsification, concealment, alteration or unauthorised destruction of records.
- Bribery, kickbacks, facilitation payments, improper gifts, secret commissions or other corrupt conduct.
- Undisclosed or improperly managed conflicts of interest and related-party concerns.
- Abuse of authority, serious dishonesty or deliberate circumvention of controls.
- Material breach of law, licence, regulatory direction, contract, Code of Conduct or Company policy.

- Suspicious or unusual financial activity, sanctions concerns or other transactions requiring specialist review.
- Misuse or unauthorised disclosure of confidential information, intellectual property or personal data.
- Serious cyber-security, privacy, health, safety, environmental or community-impact concerns.
- Obstruction of an audit or investigation, destruction of evidence, retaliation, or concealment of any covered conduct.
- Any other conduct that may cause material legal, financial, operational, safety or reputational harm.

7. Matters not covered and Alternative channels

Alternative channels are available for reporting grievances or issues relating to the following matters. Notwithstanding the availability of an alternative channel, this Policy may still apply to situations as described below.

Matter	Primary channel	When this Policy may still apply
Sexual harassment	Internal POSH Committee	Retaliation, concealment, interference with the Internal Committee, or systemic control failure may be reviewed under this Policy without replacing the POSH process.
Pay, leave, workload, appraisal or transfer grievance	HR grievance process	If the matter includes retaliation, discrimination, falsification, corruption or abuse of authority.
Routine performance or disciplinary disagreement	HR appeal or disciplinary process	For instances of deliberate process manipulation or retaliation.
Customer service issue	Customer support or grievance channel	For instances of fraud, bribery, systemic concealment or serious legal breach.
Vendor commercial dispute	Contract owner, procurement or legal	For instances of collusion, kickbacks, false records or conflict of interest.
Operational defect or suggestion	Functional escalation or incident process	If a serious safety, legal or financial risk is concealed

The EVO may redirect a matter to an alternative. Redirection does not remove protection where the original report was made in good faith.

8. Reporting channels

The Company provides the following channels for reporting a matter under this Policy.

Channel	Use
Dedicated email	Send an email to ethicstaskforce@biofuelcircle.com

Channel	Use
	This method does not support anonymous reporting.
Secure web form	Click here (www.biofuelcircle.com/whistleblower) to report Use this method for anonymous reporting. You will receive a case tracking number which will allow you to follow-up without revealing your identify
Post or Mail	Write to EVO or Audit Committee Chairperson at: BiofuelCircle Private Limited 3rd floor, Gaikwad Avenue, Off ITI Road, Aundh, Pune 411007 Mark the envelope "Private and Confidential: Vigil Mechanism" This method may be used for anonymous reporting, but is not recommended without providing a safe method for follow-up
Direct report	In person or by telephone to the EVO or Alternate EVO or Audit Committee Chairperson or nominated Director.
Exceptional direct access	A Whistleblower may contact the Audit Committee Chairperson or nominated Director directly where senior management, the EVO, retaliation, evidence suppression or a conflict is involved.

A Whistleblower does not need to report through a line manager or any other officer of the company. Whistleblowers are requested to report the matter directly through the channels provided.

9. Information to be provided

When reporting any matter, the following details should be provided:

- Description of the conduct and why it is a Concern.
- Names, roles and locations, if known.
- Dates or a reasonable time period.
- Documents, records, messages or other evidence, if available.
- Names of possible witnesses.
- Any immediate safety, evidence-destruction or retaliation risk.
- A safe method for follow-up, if the report is not anonymous.

Annexure 1: Reporting Template provides a structured method for reporting any matter

A Whistleblower shall not unlawfully obtain evidence, access records beyond authorised access, or conduct surveillance. The Company may investigate even if the report is incomplete.

10. Anonymous and confidential reports

The Company accepts anonymous reports. The EVO shall assess them on specificity, seriousness, credibility, available evidence and the ability to investigate. The Company shall not close a report only because the Whistleblower is anonymous.

The Company shall protect identity to the maximum extent permitted by law and fair process. Identity may be disclosed only to persons who need it, with the Whistleblower's consent where

practical, or where disclosure is legally required. Before a compelled disclosure, the Company will inform the Whistleblower unless prohibited by law or unsafe to do so.

The Company cannot promise absolute confidentiality. Investigation facts may reveal identity even when the Company does not disclose it.

11. Protection against retaliation

The Company prohibits retaliation against a Whistleblower, a witness, a person who assists an investigation, or a person who refuses to participate in wrongdoing.

- Termination, suspension, demotion or adverse role change.
- Punitive transfer, shift change or denial of work.
- Threats, intimidation, harassment or hostile treatment.
- Unfair appraisal, withheld promotion, training or benefits.
- Blacklisting, adverse vendor action or contract pressure.
- Isolation, doxxing, identity exposure or interference with evidence.

A person who believes retaliation has occurred shall report it through any channel. The EVO shall register a separate retaliation case. The oversight authority may order interim protection, including reporting-line changes, restricted contact, preservation of records, temporary reassignment requested by the protected person, or review of proposed employment action.

Protection does not prevent proportionate action for independent misconduct or poor performance. The decision-maker must document that the action is unrelated to the Protected Disclosure.

12. Roles and Responsibilities

The table below describes the roles and responsibilities of various entities that may be called to act under this Policy

Role	Responsibilities
Audit Committee	Approve the Policy; serve as oversight authority or appoint the oversight authority where required; review material matters; ensure resources; review effectiveness annually.
Nominated Director	Oversee the mechanism; provide direct access; review material cases; decide conflicted assignments; monitor corrective action; report to the Audit Committee.
Ethics and Vigilance Officer	Receive, register and triage reports; protect confidentiality; conduct conflict checks; preserve evidence; propose investigators; track actions; prepare anonymised reports.
Alternate EVO	Act when the EVO is unavailable, implicated or conflicted.
Investigator	Follow the written mandate; maintain independence; collect and assess evidence; protect records; report facts and findings.
Human Resources (HR)	Support protection measures and implement approved employment action. HR shall not control a case involving HR leadership or a conflict.

Role	Responsibilities
Legal and Compliance	Advise on privilege, law, regulatory reporting, privacy, evidence and procedural fairness. Legal advice shall not be used to suppress a genuine Concern.
Finance and Internal Audit	Support financial, control and forensic review where independent.
Managers	Forward potential Protected Disclosures; preserve confidentiality; prevent retaliation; do not conduct informal investigations.
All persons	Co-operate honestly, protect confidentiality, preserve evidence and avoid retaliation.

13. Intake and Preliminary Assessment

On receiving a report under the Policy, the EVO will:

- Register the report and assign a case number.
- Acknowledge within seven working days where a contact method is available.
- Assess immediate threats to people, assets, evidence, legal deadlines or operations.
- Check conflicts involving the intake team, oversight authority and proposed investigator.
- Classify the subject matter, entity, severity and required expertise.
- Decide whether to redirect, seek more information, conduct preliminary enquiry, open formal investigation, or escalate immediately.
- Document the decision and reasons.

In case of conflicts involving the intake team, the EVO or intake team will recuse themselves from the investigation by providing information as defined in the internal conflict declaration form ***Error! Reference source not found.***[i]

The EVO will aim to complete the preliminary assessment within 15 working days. The EVO may extend it for good reason and record the reason.

14. Investigation process

The investigator will:

- Issue a written investigation mandate that states allegations, scope, investigator, authority, confidentiality, reporting line and target date.
- Preserve relevant documents, devices, logs, accounts and physical evidence. Use a legal hold where required.
- Prepare an investigation plan and identify applicable policies, laws and controls.
- Collect evidence lawfully. Maintain an evidence log and chain of custody for material evidence.
- Interview the Whistleblower where possible, relevant witnesses and the Subject.
- Give the Subject a fair opportunity to respond to material allegations and evidence, unless a temporary delay is necessary to protect people or evidence.
- Assess each allegation on the balance of probabilities, unless law or a disciplinary rule requires another standard.
- Prepare a factual report. Separate evidence, findings, limitations and recommendations.

- Submit the report to the authorised reviewer.
- Track corrective and preventive actions to closure.

A detailed protocol is provided in ***Error! Reference source not found.***[ii]

The target for a standard investigation is 90 calendar days from formal opening. Complex cases may take longer. The investigator shall give a written status update and revised target to the oversight authority.

15. External investigators and Legal counsel

The oversight authority may appoint external legal counsel, a forensic firm, auditor, investigator, cyber specialist, safety specialist or other expert where independence, privilege, specialist skill, cross-border work or material exposure requires it.

The engagement letter shall define scope, reporting, confidentiality, data handling, conflicts, deliverables, privilege position and record ownership. The Company shall not appoint a person whose existing work creates a material conflict.

16. Findings and Corrective action

The authorised reviewer shall classify each allegation as substantiated, partly substantiated, unsubstantiated, inconclusive or outside scope. “Unsubstantiated” does not mean that the complaint was false.

The Company will undertake corrective action as follows:

- Disciplinary action under applicable policy and contract.
- Control, process, approval or segregation-of-duty changes.
- Recovery, insurance notification or civil action.
- Vendor suspension, remediation or termination.
- Training, supervision or policy revision.
- Safety, environmental, cyber or privacy remediation.
- Voluntary or mandatory notification to an authority.
- Root-cause analysis and testing of completed action.

The Company may tell the Whistleblower that the case is closed and whether appropriate action was taken. It shall not disclose confidential disciplinary or personal information.

17. Escalation and external reporting

The EVO shall immediately notify the oversight authority of a Material Case. The following are presumptive escalation triggers:

- Allegations against a Director, CEO, CFO, CXO team member, Secretary, EVO, senior HR or Legal leader, or member of the oversight authority.
- Suspected material fraud, bribery, financial-statement manipulation or diversion of funds.
- Immediate threat to life, health, safety, environment, critical systems or evidence.

- Likely mandatory report to a regulator, law-enforcement agency, statutory auditor or other authority.
- Retaliation by senior management or repeated retaliation.
- Cross-entity conduct or material reputation exposure.

The Company shall make external reports when required by law. This Policy does not restrict a person from lawful reporting to a government authority. A person should protect confidential and personal information and comply with lawful process.

18. Fair treatment of the Subject

An allegation is not a finding. The Company shall protect the Subject from premature judgement and unnecessary disclosure. The Subject shall co-operate, preserve evidence and avoid contact that may influence witnesses. The Subject may identify relevant evidence and provide a response.

The Company may take neutral interim measures. An interim measure is not disciplinary action and shall be reviewed regularly.

19. Good-faith, negligent and malicious complaints

In acting on complaints that may be unsubstantiated, incomplete, deficient or deviant in any fashion, the Company will be guided as follows:

Type	Treatment
Good-faith report not substantiated	Protected. No action against the Whistleblower.
Report with error or incomplete recall	Assess facts and intent. Correct the record. Do not treat an honest error as malicious.
Negligent circulation outside the mechanism	Address confidentiality or conduct concerns proportionately. Preserve protection for the underlying good-faith report.
Knowingly false or malicious report	May result in proportionate disciplinary or contractual action after a separate finding of bad faith.
Repeated frivolous complaint by director or employee	The oversight authority may take suitable action, including reprimand, as permitted by Rule 7(5).

20. Confidentiality, privacy and data handling

In handling data as part of the investigation the Company will:

- Collect only information reasonably needed for intake, investigation, legal duties and corrective action.
- Limit access by role and case assignment.
- Use secure storage, encryption where available, access logs and controlled exports.
- Not keep case files in ordinary shared folders, open email groups or personnel files.
- Share personal data between group entities only for a defined case purpose and with documented access controls.

- Apply legal holds and deletion controls.
- Report and manage any personal data breach under applicable law and applicable Company policy.
- Use local addenda for overseas entities and cross-border transfers.

The EVO and Legal function shall review the processing basis and applicable DPDP Act commencement position before high-risk or external data sharing.

21. Record keeping and retention

The EVO shall maintain a secure case register, conflict check, intake material, evidence log, interview record, investigation report, decisions, corrective-action tracker, communications and closure note.

Case records shall be retained for eight years after closure. The Company shall retain them longer where a legal hold, investigation, litigation, insurance, tax, employment or regulatory requirement applies. The Company shall suspend deletion when a preservation duty exists.

22. Governance, monitoring and reporting

The EVO shall submit a quarterly anonymised summary to the oversight authority. The summary shall not identify a Whistleblower or Subject unless needed for oversight of a Material Case.

Metric	Minimum reporting
Intake	Cases received by channel, entity and category.
Status	Open, closed, redirected and overdue cases.
Timing	Acknowledgement, assessment and investigation ageing.
Outcomes	Substantiated, partly substantiated, unsubstantiated, inconclusive and outside-scope results.
Risk	Material cases, retaliation allegations, repeat themes and control failures.
Action	Corrective actions due, overdue and verified.
Awareness	Training coverage and channel tests.
Independence	Conflicts identified and external investigators used.

The oversight authority may report significant matters to the Board. The Board may review the mechanism annually or such intervals as the Board may deem fit.

23. Group companies, subsidiaries and joint ventures

Controlled subsidiaries shall adopt this Policy as a minimum standard. Each shall nominate a local coordinator. The Group EVO shall maintain common standards, training, case numbering, investigator quality and aggregate reporting.

A complaint involving subsidiary management shall bypass local management and go to the Group EVO and parent oversight authority. A complaint involving parent management will go directly to the Audit Committee Chairperson or nominated Director.

For a jointly controlled entity, BiofuelCircle shall seek adoption through the JV Board. The JV policy should provide an independent channel that is not controlled by only one shareholder. Cross-entity investigations will require a written mandate, agreed data access, confidentiality rules and clear decision rights.

An overseas group entity shall use a local addendum where local employment, privacy, whistleblowing, works council or regulatory law requires it. The stricter lawful protection shall apply.

24. Awareness, Training and Communication

The Company will:

- Publish the Policy and current reporting channels on the intranet and, for external stakeholders, on the website or supplier portal.
- Include the Policy in joining and contractor induction.
- Ask existing employees and contractors on the date of first adoption of the policy to undergo mandatory training on the Policy
- Train managers to recognise and forward Protected Disclosures.
- Train the EVO, investigators, HR, Legal and oversight authority on conflicts, evidence, interviewing, privacy and retaliation.
- Test each channel at least annually.
- Communicate non-retaliation and examples of matters covered and excluded.

25. Policy review and amendment

The Audit Committee shall review this Policy at least annually and earlier after a material legal change, significant case, control failure, restructuring, new jurisdiction or Board direction. The Policy owner may make non-substantive contact or formatting updates. The Audit Committee shall approve substantive changes.

26. Effective date and interpretation

This Policy is effective from 26 August 2026. The Audit Committee has final authority to interpret it, subject to applicable law. If this Policy conflicts with mandatory law, the law applies and the remaining provisions continue.

Annexure 1: Reporting Template

Field	Information
Preferred Name or Anonymous	
Safe contact method	Phone number or Email, either one is mandatory
Entity and location	
Nature of Concern	Choose one of twelve categories (see below)
What happened	
Persons involved	
Dates or period	
Evidence available	
Witnesses	
Immediate risk	
Previous report made (if any)	

Do not investigate the matter yourself
Provide information that you already hold lawfully. Do not access records beyond your authority or confront the Subject.

Selections for Nature of Concern:

- Fraud, Theft & Misappropriation
- Financial & Accounting Manipulation
- Falsification & Record Tampering
- Bribery, Corruption & Improper Payments
- Conflicts of Interest & Related Party Concerns
- Abuse of Authority & Control Breaches
- Legal, Regulatory & Policy Violations
- Suspicious Financial Activity & Unusual Transactions
- Confidentiality, IP & Data Misuse
- Cybersecurity, Health, Safety & Environmental Concerns
- Obstruction, Evidence Tampering & Retaliation
- Other Serious Misconduct or Harm / None of the Above

Note

[i] Annexure 6 in an internal conflict declaration form
[ii] Annexure 3 is an internal investigation protocol

Annexures 2 to 6 are controlled internal procedures and templates. Their omission from this public version does not limit any reporting right or protection under this Policy.