

Whistleblower and Non-Retaliation Policy

Kovon Global Private Limited | Level 1 Board Policy

Policy owner	Head of People
Approving authority	Board of Directors
Effective date	1 April 2026
Version	1.0
Review frequency	Annual, or earlier if required by law, serious incident, audit finding or Board direction
Primary jurisdiction	Bengaluru, India
Applies to	Employees, interns, consultants, contractors, agency workers, directors, officers, vendors, candidates, clients, placement partners and other persons who report concerns involving Kovon
Reporting channel	ethics@kovon.io
Board escalation contact	Board Chair
Related policies	Corporate Policy Governance Framework; Code of Conduct and Ethics Policy; POSH framework and Internal Committee process; Data Privacy and Information Security policies once adopted

Board commitment

Kovon encourages good-faith reporting of suspected misconduct and prohibits retaliation. Concerns involving senior management, fraud, corruption, harassment, privacy, security or material legal risk must be handled with independence, confidentiality and appropriate Board visibility.

1. Purpose

Kovon Global Private Limited ("Kovon" or the "Company") adopts this Whistleblower and Non-Retaliation Policy to provide safe, reliable and confidential channels for reporting suspected misconduct, legal violations, unethical conduct, fraud, retaliation or serious policy breaches.

The policy is intended to protect people who raise concerns in good faith, ensure concerns are assessed fairly, and give the Board of Directors appropriate visibility over serious matters that may affect Kovon's integrity, legal compliance, workforce trust or reputation.

2. Scope

This policy applies to concerns raised by or involving:

1. employees, interns, trainees and apprentices;
2. consultants, contractors, advisors and freelancers;
3. agency workers and vendor-deployed personnel;
4. directors, officers and managers;
5. vendors, clients, candidates, placement partners, workers, business partners or third parties who have a work-related concern involving Kovon.

External parties may report under this policy where the concern involves Kovon people, Kovon systems, recruitment conduct, candidate payments, fraud or retaliation.

This policy does not replace normal management feedback, HR support, performance discussions, payroll queries or routine workplace complaints unless the concern involves suspected misconduct, retaliation, illegality, fraud, harassment, discrimination, abuse of authority or serious policy breach.

3. Reportable Concerns

Reportable concerns include actual, suspected or attempted conduct involving:

6. fraud, theft, falsification of records, misappropriation or misuse of company assets;
7. bribery, corruption, kickbacks, improper gifts, secret commissions or improper candidate/vendor payments;
8. harassment, sexual harassment, discrimination, bullying, intimidation or abuse of authority;
9. retaliation against a person for raising a concern, refusing misconduct or cooperating with a review;
10. privacy breaches, unauthorised data access, information security incidents or misuse of candidate/client data;
11. conflicts of interest, related-party conduct or favouritism that is concealed or unmanaged;
12. serious breach of law, regulation, contract or Kovon policy;
13. unsafe practices, threats, violence or conduct that may endanger people;
14. deliberate concealment, destruction of evidence or obstruction of an investigation.

4. Good-Faith Reporting

A report is made in good faith when the person reasonably believes the concern may be true and provides information honestly, even if the concern is later not substantiated.

A person does not need proof before reporting. However, knowingly false, malicious, fabricated or bad-faith reports may be treated as misconduct.

5. Reporting Channels

Kovon's designated whistleblower reporting channel is ethics@kovon.io. Concerns may also be reported to:

15. the person's manager or skip-level manager, unless the manager is involved in the concern;
16. Head of People;
17. Legal / Compliance or designated compliance contact;
18. Kovon's Internal Committee under POSH for sexual harassment matters;
19. the CEO, as the default investigation owner;
20. the Board Chair for concerns involving senior management, fraud, retaliation, corruption, material legal risk or suspected concealment.

Implementation action

Kovon should configure ethics@kovon.io with restricted access, create a matching HRMS / employee portal case category where feasible, and publish the channel clearly for covered persons and relevant external parties.

6. Anonymous Reporting

Kovon allows anonymous reports where legally permissible and operationally feasible. Anonymous reports should include enough detail to allow assessment, such as dates, persons involved, documents, communications, systems, transactions or witnesses.

Anonymous reporting can limit Kovon's ability to seek clarification, provide updates or fully investigate. Kovon will nevertheless assess anonymous reports based on the information available.

7. Confidentiality

Kovon will handle whistleblower reports sensitively and share information only with persons who need to know for intake, triage, investigation, remediation, legal advice, Board oversight, disciplinary action or compliance with law.

Confidentiality does not mean absolute secrecy. Kovon may need to disclose limited information to conduct a fair investigation, protect people, preserve evidence, provide due process, comply with legal obligations or take corrective action.

8. Non-Retaliation

Kovon prohibits retaliation against any person who, in good faith, raises a concern, seeks guidance, refuses to participate in suspected misconduct, assists an investigation, provides evidence or exercises a legal right.

Retaliation may include

Examples

Employment or engagement action	Termination, demotion, suspension, reduced work, denial of promotion, unfavourable shift or assignment changes.
Managerial or peer conduct	Threats, intimidation, exclusion, humiliation, bullying, harassment, pressure to withdraw a report.
Performance or opportunity impact	Unfair rating, blacklisting, removal from projects, denial of learning or client opportunities.
Contractor or vendor impact	Improper non-renewal, payment delay, access restriction or commercial penalty because a concern was raised.

Any suspected retaliation must be reported immediately. Retaliation may result in disciplinary action up to and including termination of employment or engagement.

9. Intake and Triage

Upon receiving a report, the authorised intake owner should record the concern, assess urgency, preserve relevant evidence and determine the appropriate review path.

Concern type	Default handling path
Senior management, Board-level conflict, fraud, corruption or material legal risk	Escalate to the Board Chair and Legal / Compliance where available.
Sexual harassment	Route to Kovon's Internal Committee under POSH and handle under the POSH process.
Privacy or information security incident	Escalate to privacy/security owner and Legal / Compliance; preserve logs and access evidence.
HR, conduct or workplace misconduct	Head of People to triage and assign reviewer independent of the alleged conduct.
Finance, expense, payroll or vendor concern	Finance and Legal / Compliance review, with Board escalation for material issues.

10. Investigation Principles

The CEO is the default investigation owner for whistleblower matters, except where the CEO is conflicted, implicated, unavailable or where Board-level independence is required. In those cases,

the Board Chair will appoint an appropriate reviewer, which may include external counsel or an independent investigator.

Investigations must be fair, timely, independent of the alleged misconduct where practical, evidence-based and respectful of confidentiality and due process.

21. The reviewer should define the issue, scope, records to be preserved, persons to be interviewed and expected timeline.
22. Persons accused of misconduct should be given a fair opportunity to respond where appropriate and legally permissible.
23. Investigations should be documented, including findings, evidence reviewed, credibility considerations, conclusions and recommended action.
24. Where specialist expertise is required, Kovon may appoint external legal, forensic, HR, security or compliance advisors.
25. Investigation records must be retained under the document retention rules in the Corporate Policy Governance Framework.

11. Evidence Preservation and Cooperation

Covered persons must preserve relevant documents, messages, logs, devices, files, financial records and other evidence when they become aware of a report or investigation. Deleting, altering, concealing or fabricating evidence is prohibited.

Covered persons are expected to cooperate honestly with authorised reviews and investigations. Interference, witness coaching, intimidation, refusal to cooperate without valid reason or false statements may lead to disciplinary or contractual action.

12. Feedback to Reporter

Where the reporter's identity and contact details are known, Kovon will acknowledge receipt within 7 working days and may provide reasonable status updates, subject to confidentiality, privacy, legal privilege, employee rights and investigation integrity.

Kovon may not be able to share detailed findings, disciplinary decisions or personal information about other individuals.

13. Target Timelines

Kovon will seek to manage whistleblower reports within the following target timelines, recognising that complex, sensitive, cross-border, forensic, legal or multi-party matters may require more time:

Stage	Target timeline
Acknowledgement	Within 7 working days where reporter contact details are available.

Initial triage	Within 10 working days of receipt.
Investigation closure	Normally within 45 to 60 days, depending on complexity, evidence availability, legal requirements and participant availability.
Remediation tracking	Action owners and target dates should be recorded for substantiated concerns requiring corrective action.

14. Corrective and Disciplinary Action

If a concern is substantiated, Kovon will determine corrective action based on severity, legal requirements, impact, intent, seniority, prior conduct and remediation needs.

- 26. disciplinary action, including warning, suspension, termination or contract action;
- 27. process, control, training or policy changes;
- 28. recovery of funds or correction of records where legally permitted;
- 29. restriction or removal of system access;
- 30. vendor, client or partner action;
- 31. reporting to regulators or law enforcement where required or appropriate.

15. Reporting to the Board

The CEO, Head of People, Legal / Compliance or Board-designated reviewer must provide the Board Chair with appropriate visibility over serious whistleblower matters. Board reporting should protect confidentiality while enabling oversight.

Board reporting may include number and type of concerns, ageing, substantiation rate, material matters, retaliation allegations, repeat themes, remediation status and overdue actions.

16. Protection of Personal Data

Whistleblower records may contain sensitive personal information. Kovon will process such information only for legitimate reporting, investigation, compliance, legal, disciplinary, audit and governance purposes. Access must be limited to authorised persons with a need to know.

17. Relationship with Other Policies and Rights

This policy works alongside the Code of Conduct and Ethics Policy, Kovon's POSH framework and Internal Committee process, Data Privacy Policy once adopted, Information Security Policy once adopted, employment contracts and applicable law.

Nothing in this policy prevents a person from exercising statutory rights, reporting to lawful authorities where permitted, participating in legal proceedings or seeking legal advice.

18. Misuse of the Policy

Kovon will not discipline a person merely because a good-faith concern is not substantiated. However, knowingly false, malicious, fabricated or bad-faith allegations, or misuse of the reporting process to harass or harm another person, may result in disciplinary or contractual action.

19. Acknowledgement

Acknowledgement of this policy is mandatory for all covered persons. Kovon will capture acknowledgements through the HRMS / employee portal or another approved evidence method. Failure to acknowledge does not excuse non-compliance where the policy has been validly issued and made available.

20. Review and Amendment

This policy will be reviewed annually by the Head of People and submitted to the Board of Directors for approval of material changes. Earlier review may be triggered by legal change, serious incident, audit finding, investigation trend or Board direction.

Appendix A: Report Intake Checklist

The intake owner should record the following where available:

32. date and time of report;
33. reporting channel used;
34. reporter name and contact details, if provided;
35. persons or functions involved;
36. summary of allegation or concern;
37. dates, locations, systems, transactions or documents involved;
38. immediate safety, data, access or retaliation risk;
39. evidence preservation steps taken;
40. triage decision, assigned reviewer and escalation path;
41. target review date and closure status.

Appendix B: Acknowledgement

I acknowledge that I have received or been given access to Kovon's Whistleblower and Non-Retaliation Policy. I understand that I may raise concerns in good faith, that retaliation is prohibited, and that I am expected to cooperate honestly with authorised reviews and investigations.

Name	
Role / engagement type	
Department / function	
Signature / electronic acknowledgement	
Date	