Kovon Global Private Limited
Reg Office: Flat No. C-602, Mana, Uber Verdant Phase 2, Carmelram, Bangalore, Bangalore South, Karnataka, India, 560035

CIN: U62099KA2025PTC204920

Corporate Policy Governance Framework

Kovon Global Private Limited | Bengaluru, India

Document 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, business change, audit findings or Board direction
Applies to	Employees, interns, consultants, contractors and agency workers engaged by Kovon Global Private Limited
Publication	HRMS / employee portal

Board governance note

This framework is intended to create a controlled, auditable system for creating, approving, publishing, acknowledging, reviewing and enforcing Kovon's employment, conduct, risk and operating policies.

1. Purpose

Kovon Global Private Limited ("Kovon" or the "Company") adopts this Corporate Policy Governance Framework to ensure that all company policies are legally conscious, consistently owned, clearly approved, accessible to the workforce and periodically tested for effectiveness.

The framework should be read as the parent governance document for Kovon's employee policies and related standards. Individual policies must align with this framework unless the Board of Directors approves a specific deviation or applicable local law requires a different approach.

2. Scope

This framework applies to all Kovon policies, standards, SOPs, control procedures, forms and addenda that regulate the conduct, obligations, rights, benefits, access, risk management or working practices of:

1. full-time and part-time employees;
2. interns, apprentices and trainees;
3. consultants, independent contractors and advisors;

4. agency workers, vendor-deployed personnel and other contingent workers; and
5. any other person who is given access to Kovon's systems, data, facilities, candidates, customers or confidential information.

Where the terms of a contract, statement of work or vendor arrangement are more restrictive than this framework, the more restrictive obligation will apply, subject always to applicable law.

3. Governance Principles

Legality: Policies must comply with applicable Indian law and any mandatory local law in the jurisdictions where Kovon operates or engages workers.

Board visibility: Policies that materially affect legal liability, ethics, risk, privacy, information security or stakeholder trust must be approved by the Board.

Operational usability: Policies must be written in plain, enforceable language that managers, HR, employees and covered workers can apply consistently.

Single source of truth: The HRMS / employee portal is the authoritative publication location for current policies.

Evidence and auditability: Kovon must be able to evidence approvals, acknowledgements, exceptions, reviews, training and disciplinary outcomes.

Local-law adaptability: Global or company-wide policies may be supplemented by jurisdiction-specific addenda where local requirements differ.

4. Policy Hierarchy

Kovon will maintain a four-level policy hierarchy. A lower-level document must not contradict a higher-level document unless the exception is expressly approved and documented.

Level	Document type	Primary authority	Typical examples
Level 1	Board policies	Board of Directors	Code of Conduct, Whistleblower Policy, Data Privacy Policy, Information Security Policy, Anti-Bribery and Anti-Corruption Policy, Related Party Conduct Policy.
Level 2	Company-wide employee policies	Board or management, based on risk	Employee Handbook, Leave Policy, Remote Work Policy, POSH Policy, Travel and Expense Policy,

Level	Document type	Primary authority	Typical examples
			Performance Management Policy.
Level 3	Departmental standards	Functional head with People/Legal review	Engineering standards, recruitment operations standards, sales conduct standards, candidate support standards, finance controls, global mobility standards.
Level 4	SOPs and control procedures	Process owner with functional approval	Approval matrices, checklists, workflow documents, onboarding forms, access request procedures, incident reporting forms.

5. Policy Ownership and Approval

Every policy must have a named policy owner. The policy owner is accountable for drafting, consultation, implementation, training coordination, review, exception tracking and evidence retention.

Role	Core responsibilities
Board of Directors	Approve Level 1 policies and any other policy the Board reserves to itself; review material breaches, audit outcomes and management certifications where appropriate.
Head of People	Own this framework; maintain the policy register; coordinate policy publication, acknowledgements, workforce communication and annual review cycles.
Legal / Compliance	Review policies for legal risk, mandatory language, enforceability, regulatory sensitivity and local-law addenda where required.

Role	Core responsibilities
Information Security / Privacy Owner	Review policies affecting systems, data, access, monitoring, security controls, incident response or personal information.
Functional heads	Own department standards and SOPs within their area; ensure operational controls match approved company policy.
Managers	Apply policies consistently, escalate exceptions and breaches, and ensure covered workers understand relevant obligations.
Covered workforce	Read, acknowledge and comply with applicable policies and report suspected breaches through approved channels.

6. Board-Approved versus Management-Approved Policies

The following policies require Board approval because they may materially affect legal liability, ethical conduct, risk posture, privacy, information security, stakeholder trust or statutory compliance:

6. Code of Conduct and Ethics;
7. Whistleblower and Non-Retaliation Policy;
8. Anti-Bribery, Anti-Corruption and Gifts Policy;
9. Data Privacy and Personal Information Protection Policy;
10. Information Security and Acceptable Use Policy;
11. Related Party Conduct and Conflict of Interest Policy;
12. Prevention of Sexual Harassment (POSH) Policy;
13. Disciplinary Policy and breach consequence framework;
14. Delegation of Authority / approval matrix where financial or legal authority is assigned; and
15. any policy specifically escalated by the CEO, Head of People, Legal / Compliance or Internal Audit.

Management may approve lower-risk Level 2 policies, Level 3 departmental standards and Level 4 SOPs, provided they remain consistent with Board-approved policies and are reviewed by the required control functions.

7. Policy Lifecycle

Kovon will use the following lifecycle for new and revised policies:

16. Need identification: The policy owner identifies the business, legal, workforce or control need.
17. Drafting: The policy owner prepares a draft using Kovon's approved policy template and plain-language drafting standards.
18. Stakeholder review: HR, Legal / Compliance, Finance, Information Security, Privacy and affected functional heads review as applicable.
19. Approval: The policy is submitted to the correct approving authority based on the policy hierarchy and risk classification.
20. Publication: The final approved policy is published on the HRMS / employee portal as the single source of truth.
21. Acknowledgement and training: Covered workers acknowledge the policy, and targeted training is completed where required.
22. Monitoring: The policy owner monitors implementation, exceptions, questions, breaches and audit findings.
23. Review and refresh: The policy is reviewed annually or sooner if triggered by law, business change, incident, audit finding or Board direction.

8. Version Control and Policy Register

The Head of People must maintain a central policy register. At minimum, the register should record the policy title, level, owner, approving authority, effective date, version, last review date, next review date, publication location, acknowledgement requirement and status.

Control	Requirement
Version numbering	Use major and minor version control, such as 1.0 for the first approved issue and 1.1 for non-material updates.
Change log	Every policy must include or link to a change log summarising material changes, approval date and approver.
Archived policies	Superseded versions must be retained but removed from active employee-facing publication areas.
Draft control	Drafts must be watermarked or clearly marked as draft and must not be published as enforceable policy.

9. Employee Acknowledgement Process

Kovon will require acknowledgement for all Board-approved policies and any company-wide employee policy that imposes obligations on covered workers.

24. Acknowledgements should be captured through the HRMS / employee portal wherever feasible.
25. New joiners should complete policy acknowledgements during onboarding before or shortly after system access is granted.
26. Existing covered workers should acknowledge new or materially revised policies within the timeline communicated by HR.
27. Managers are responsible for following up on overdue acknowledgements within their teams.
28. Failure to acknowledge a policy does not excuse non-compliance where the policy was validly published and communicated.

10. Policy Exceptions

Exceptions must be rare, time-bound, risk-assessed and documented. No exception may waive mandatory legal requirements, statutory rights, anti-harassment protections, privacy obligations, information security minimums or Board-reserved controls without the required legal and Board-level review.

Exception element	Minimum requirement
Request	Submitted by the business owner or manager with business rationale, impacted workers, duration and proposed controls.
Review	Reviewed by the policy owner and relevant control function, such as Legal / Compliance, People, Finance, Privacy or Information Security.
Approval	Approved by the authority specified in the policy or, if not specified, by the policy owner plus the relevant functional head. Board policy exceptions require Board or Board-delegated approval.
Expiry	Every exception must have an expiry date and must be reassessed before renewal.
Recordkeeping	The Head of People or policy owner must retain an exception log for audit and review.

11. Breach Reporting and Consequences

Suspected policy breaches must be reported promptly through the appropriate reporting channel, which may include the manager, Head of People, Legal / Compliance, designated grievance mechanism, whistleblower channel or POSH committee, depending on the nature of the issue.

Consequences must be proportionate, consistent, evidence-based and compliant with applicable law and contractual rights. Depending on severity, a breach may result in counselling, retraining, written warning, loss or restriction of access, repayment or recovery where legally permitted, termination of engagement, referral to authorities or civil/criminal action.

Retaliation against a person who raises a concern in good faith is prohibited and may itself be treated as a serious breach.

12. Local-Law Addenda and Conflict Rules

Kovon's primary jurisdiction for this framework is Bengaluru, India. As Kovon expands or engages workers in other locations, the Company may issue local-law addenda to reflect mandatory employment, tax, privacy, social security, working time, leave, health and safety or contractor classification requirements.

If a global or company-wide policy conflicts with applicable local law, local law will prevail to the extent of the conflict. The policy owner must document the conflict, obtain Legal / Compliance review and issue a local-law addendum or corrective communication as appropriate.

13. Document Retention

Kovon must retain policy governance records for a period consistent with applicable law, contractual obligations, litigation hold requirements and internal records schedules. Unless a stricter rule applies, policy records should be retained for the life of the policy plus at least seven years.

29. approved policy versions and Board or management approvals;
30. policy register and change logs;
31. acknowledgement records and training completion records;
32. exception requests, approvals and expiry evidence;
33. breach investigations, disciplinary records and remediation evidence; and
34. audit reports, management responses and closure evidence.

14. Internal Audit and Compliance Testing

The Head of People, in coordination with Legal / Compliance and Internal Audit or an appointed reviewer, should conduct periodic compliance testing. The testing program should be risk-based and may include:

35. policy register completeness and approval evidence;
36. sample testing of employee acknowledgements;

37. review of overdue policy reviews and expired exceptions;
38. testing of high-risk policies such as privacy, information security, POSH, whistleblowing and expense controls;
39. review of breach handling consistency and remediation closure; and
40. Board reporting on significant gaps, high-risk exceptions and repeat breaches.

15. Publication and Communication

The HRMS / employee portal is Kovon's authoritative policy publication channel. HR may also circulate launch communications, manager talking points, FAQs, training links and acknowledgement reminders, but those communications do not replace the approved policy text.

Policies must be organised so workers can find them easily by category, effective date and applicability. Withdrawn or superseded policies should not remain visible in active policy folders.

16. Review, Certification and Amendment

This framework will be reviewed annually by the Head of People and presented to the Board of Directors for approval of material changes. Non-material administrative updates, such as formatting, owner title updates or publication link corrections, may be made by the Head of People if they do not alter rights, obligations, controls or approval authority.

Each annual review should include a certification that the policy register has been reviewed, high-risk policies are current or on a remediation plan, exceptions have been reviewed and material compliance gaps have been escalated.

Kovon Global Private Limited
Reg Office: Flat No. C-602, Mana, Uber Verdant Phase 2, Carmelram, Bangalore, Bangalore South, Karnataka, India, 560035

CIN: U62099KA2025PTC204920

Appendix A: Recommended Policy Roadmap

The following roadmap identifies the next policies Kovon should draft under this hierarchy. The sequence is designed to prioritise legal exposure, workforce trust, information security, candidate/customer data and management consistency.

Priority	Policy	Level	Recommended approver	Why it matters
1	Code of Conduct and Ethics	1	Board	Sets the behavioural baseline for integrity, respect, confidentiality, conflicts and company reputation.
2	Whistleblower and Non-Retaliation Policy	1	Board	Creates protected channels for reporting serious misconduct and supports Board oversight.
3	POSH Policy	1	Board	Supports statutory compliance and a safe workplace for employees and covered workers in India.
4	Data Privacy and Candidate Data Protection Policy	1	Board	Protects personal data of employees, candidates, customers and business partners.
5	Information Security and Acceptable Use Policy	1	Board	Defines access, device, password, monitoring, data handling and incident obligations.
6	Anti-Bribery, Gifts and Anti-Corruption Policy	1	Board	Controls interactions with clients, vendors, candidates, public officials and business partners.
7	Related Party Conduct and Conflict of Interest Policy	1	Board	Prevents undisclosed personal benefit, biased hiring/vendor decisions and related-party risk.
8	Employee Handbook / Conditions of Employment	2	Board or CEO with Board noting	Collects core employment rules, workplace expectations and policy links.
9	Leave, Holidays and Attendance Policy	2	Management	Creates consistent working time, absence, holiday and attendance administration.
10	Remote / Hybrid Work Policy	2	Management	Sets expectations for availability, data security, work location and equipment.

Priority	Policy	Level	Recommended approver	Why it matters
11	Compensation, Benefits and Payroll Governance Policy	2	Management with Finance	Supports consistent pay practices, payroll cut-offs, benefits eligibility and approvals.
12	Performance Management and Promotion Policy	2	Management	Creates fair cycles for goal setting, feedback, ratings, promotion and performance improvement.
13	Disciplinary and Grievance Policy	2	Board or Management with Legal	Defines due process, escalation, investigation and consequences.
14	Travel, Expense and Reimbursement Policy	2	Management with Finance	Controls business spend, documentation, approvals and reimbursement timelines.
15	Recruitment Operations Standard	3	Head of Talent / People	Standardises requisitions, candidate communication, interviews, offer approvals and candidate records.
16	Engineering Secure Development Standard	3	CTO / Security	Defines code, access, review, secrets management, deployment and incident practices.
17	Candidate Support and Service Quality Standard	3	Operations Head	Controls candidate-facing response standards, complaint handling and escalation.
18	Vendor and Contractor Onboarding SOP	4	Process owner	Ensures NDA, access, background checks, data controls and offboarding are completed.

Appendix B: Minimum Policy Template

Each Kovon policy should use a consistent template. At minimum, every policy should include:

41. policy title, version, effective date and owner;
42. approving authority and approval date;
43. scope and covered persons;
44. policy statement and required standards of conduct;
45. roles and responsibilities;
46. process steps, where relevant;

47. exceptions and approval path;
48. breach reporting and consequences;
49. related policies, SOPs, forms and local-law addenda;
50. review frequency and change log.

Appendix C: Initial Implementation Checklist

51. Approve this framework through the Board of Directors.
52. Create the central policy register owned by the Head of People.
53. Confirm the standard policy template and naming convention.
54. Classify existing and planned policies into Levels 1 to 4.
55. Identify which existing documents require Board approval or re-approval.
56. Publish current policies on the HRMS / employee portal.
57. Launch acknowledgement campaigns for Board-approved and company-wide policies.
58. Create an exception log and breach register.
59. Schedule annual review dates and assign policy owners.
60. Report first-cycle implementation status to the Board.