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

CIN: U62099KA2025PTC204920

Information Security and Acceptable Use Policy

Kovon Global Private Limited | Level 1 Board Policy

Policy owner	CTO / Security Owner
Executive accountability	CEO
Operational stakeholders	IT Admin, Engineering Head, Head of People and functional heads
Approving authority	Board of Directors
Effective date	1 April 2026
Version	1.0
Review frequency	Annual, or earlier after a material incident, audit finding, system change, product change or Board direction
Primary jurisdiction	Bengaluru, India
Security contacts	privacy@kovon.io and ethics@kovon.io
Applies to	Employees, interns, contractors, agency workers, consultants, vendors and any person with access to Kovon systems, data, code, devices or accounts
Related policies	Corporate Policy Governance Framework; Code of Conduct and Ethics Policy; Data Privacy and Candidate Data Protection Policy; Whistleblower and Non-Retaliation Policy

Security standard

Kovon systems, candidate data, client information, source code, credentials and business records must be protected through least privilege, approved systems, secure devices, careful communication and prompt incident reporting.

1. Purpose

Kovon Global Private Limited ("Kovon" or the "Company") adopts this Information Security and Acceptable Use Policy to protect company systems, personal data, candidate and client information, source code, credentials, business records and technology assets.

This policy sets minimum controls for access, devices, passwords, remote work, acceptable use, WhatsApp and personal messaging, AI tools, software development, monitoring and security incident reporting.

2. Scope

This policy applies to all persons who access Kovon systems, data, devices, accounts, communication channels, repositories, cloud environments or workplace technology. It applies whether access occurs from a Kovon office, remote location, client or vendor location, personal device, company device or mobile device.

Core systems covered by this policy include Kovon HRMS, ATS, Microsoft 365, CRM, cloud databases, GitHub/code repositories, payroll systems, background verification vendor systems, WhatsApp, website/app admin panels and any other system approved for Kovon business.

3. Security Governance and Responsibilities

Role	Responsibilities
Board of Directors	Approve this policy and receive escalation for material incidents, systemic control failures or high-risk exceptions.
CEO	Executive accountability for information security risk and escalation of material incidents.
CTO / Security Owner	Own day-to-day security controls, incident coordination, access standards, technical safeguards and security reviews.
IT Admin	Administer approved tools, accounts, endpoint controls, access changes and device support.
Engineering Head	Own engineering security practices, repository controls, secrets management, production access and secure development standards.
Head of People	Support joiner-mover-leaver controls, HR/candidate-data access approvals, training and disciplinary coordination.
Functional heads	Approve business need for access and ensure team compliance.
Covered users	Use systems responsibly, protect credentials and data, report incidents promptly and follow this policy.

4. Acceptable Use

Kovon systems and accounts must be used primarily for legitimate company work. Limited incidental personal use may be permitted if it does not interfere with work, create cost, expose Kovon to risk, violate law or policy, or compromise security.

Users must not use Kovon systems, accounts, devices, networks or data for:

1. illegal activity, harassment, discrimination, threats or abusive conduct;
2. piracy, copyright infringement, malware, unauthorised scanning or hacking;

3. credential sharing, account sharing or bypassing security controls;
4. unauthorised scraping, data harvesting, bulk exports or shadow databases;
5. crypto mining or other resource-intensive non-business activity;
6. offensive, sexually explicit, hateful or violent content unrelated to legitimate work;
7. personal commercial activity or outside work without approval;
8. unauthorised disclosure, copying or transfer of Kovon, candidate, client, employee or vendor data.

5. Access Management

Access to Kovon systems must follow least privilege, need-to-know and role-based access principles. Access must be approved before provisioning and removed when no longer required.

Control	Requirement
Access approval	Functional head plus CTO / Security Owner approval. HR/candidate-data systems also require Head of People involvement.
New joiners	Access may be granted only after approved onboarding and role-based need is confirmed.
Role changes	Access must be reviewed within 5 working days of role, department, reporting-line or responsibility change.
Leavers	Access must be disabled on the last working day. For involuntary exits or high-risk cases, access must be disabled immediately.
Privileged access	Admin, production, payroll, HRMS, ATS, CRM, cloud, code repo and website/app admin access must be tightly restricted and logged where feasible.
Shared accounts	Shared accounts are prohibited unless approved for a defined technical reason with compensating controls.

6. Access Reviews

The CTO / Security Owner, IT Admin and relevant functional heads must conduct access reviews at a cadence proportionate to risk.

System type	Review cadence
High-risk systems	Quarterly. Includes HRMS, ATS, payroll, cloud databases, GitHub/code repositories, CRM, admin tools and systems containing candidate, employee, client, financial or production data.
Standard business systems	Semi-annual. Includes lower-risk collaboration and workflow systems.

Privileged/admin access	Quarterly or after any material incident, role change, restructuring or vendor change.

7. Passwords and MFA

Users must maintain strong, unique passwords and must not share credentials. Passwords must not be stored in plain text, chat messages, documents, tickets, spreadsheets, code, screenshots or email.

Multi-factor authentication is mandatory for email, HRMS, ATS, CRM, cloud systems, code repositories and admin tools. MFA should also be enabled for other systems where available.

Suspected credential compromise, phishing, unusual login prompts or MFA fatigue attacks must be reported immediately.

8. Device Security and BYOD

Kovon permits bring-your-own-device (BYOD) access where approved and where minimum safeguards are followed. Company data on personal devices remains subject to Kovon's security and confidentiality requirements.

BYOD and company devices used for Kovon work must have:

9. screen lock with password, PIN, biometric or equivalent control;
10. updated operating system, browser and critical security patches;
11. antivirus, EDR or equivalent protection where feasible;
12. device encryption where feasible;
13. no family, friend or shared use for Kovon work profiles, files, systems or accounts;
14. remote wipe or selective wipe capability for company data where feasible and lawful;
15. secure backup, storage and disposal practices for company data.

9. Remote Work Controls

Remote work must be performed in a way that protects Kovon information and personal data. Users must use private workspaces where feasible, secure Wi-Fi, VPN if provided, and approved systems for storage and communication.

16. Do not use public or shared computers for Kovon work.
17. Avoid discussing confidential matters where conversations can be overheard.
18. Use screen privacy and lock devices when unattended.
19. Avoid printing confidential information unless necessary and approved.
20. Securely shred or dispose of printed materials containing Kovon, candidate, employee, client or vendor information.

21. Do not leave devices or documents unattended in vehicles, public places or shared accommodation.

10. Data Handling and Storage

Kovon data must be stored in approved systems wherever feasible. Users must avoid unmanaged local downloads, personal cloud storage, personal email forwarding, unauthorised spreadsheets and uncontrolled copies of candidate, employee, client or business data.

High-risk candidate or employee data, including IDs, bank details, medical records, background verification data, credentials, passport, visa documents, Aadhaar, PAN or bulk records, must be handled only through approved secure channels and access-controlled systems.

11. WhatsApp and Personal Messaging

WhatsApp may be used only for limited coordination where business need exists and where the information shared is low-risk. WhatsApp must not become the primary system of record for candidate, employee, client, financial, legal, payroll, security or high-risk operational data.

Users must not share high-risk candidate documents, IDs, bank details, medical records, credentials, bulk candidate data, source code, production information, access tokens or confidential client data through WhatsApp or personal messaging channels.

12. AI Tools and Unapproved Applications

Users must not enter confidential, candidate, client, employee, source code, credentials, personal data, high-risk data or non-public business information into unapproved public AI tools or unapproved applications.

AI tools and automation used for recruitment, matching, support, engineering, analytics or business workflows must be reviewed for privacy, security, confidentiality, vendor terms, data retention, bias and human oversight before use.

The CTO / Security Owner may maintain an approved-tools list. If a tool is not clearly approved, users must ask before using it with Kovon data.

13. Source Code, Engineering and Production Security

Kovon's code repositories and production systems are high-risk assets. Engineering and product teams must apply secure development and change-control practices.

22. branch protection for important repositories and production branches;
23. peer code review before merge or deployment, except approved emergency changes;
24. least-privilege access to repositories, environments, databases and production systems;
25. secrets management through approved tools and no hardcoded credentials, API keys or tokens;

26. logging and monitoring for important production, admin and security events where feasible;
27. separation of development, test and production environments where practical;
28. prompt patching of critical vulnerabilities and dependency risks;
29. removal of access for departed users, inactive accounts and unused integrations.

14. Email, Phishing and Communications Security

Users must exercise caution with links, attachments, payment requests, credential prompts, MFA prompts, impersonation attempts and urgent or unusual instructions. Suspicious emails, messages or calls must be reported promptly.

Users must verify unusual requests involving payments, bank details, candidate documents, payroll changes, system access, password resets, source code, confidential data or executive instructions through a trusted second channel.

15. Security Incident Reporting

Suspected security incidents must be reported immediately to privacy@kovon.io, ethics@kovon.io, the CTO / Security Owner or IT Admin. Incidents involving phishing, lost device, credential compromise, data leak or system breach should ideally be reported within 1 hour of discovery.

Incident example	Immediate user action
Phishing or suspicious link	Do not click further; report the message; preserve headers/screenshots where possible.
Lost or stolen device	Report within 1 hour where feasible; provide device, account and data details.
Credential compromise	Report immediately; change password only as instructed if investigation requires preservation.
Misdirected data or leak	Report recipients, data categories, time, channel and corrective steps already taken.
Malware or unusual system behaviour	Disconnect from network if advised; do not delete evidence; contact IT/Security.
Unauthorised code, cloud or admin access	Escalate immediately to CTO / Security Owner and Engineering Head.

16. Incident Response and Escalation

The CTO / Security Owner will coordinate technical response with IT Admin, Engineering Head, Privacy Owner / CEO, Head of People and other stakeholders as needed. Material incidents must be escalated to the CEO and, where appropriate, the Board.

Incident response should include containment, evidence preservation, impact assessment, affected-system review, user and vendor coordination, legal/privacy assessment, remediation, lessons learned and control updates.

17. Monitoring and No Expectation of Unrestricted Privacy

Kovon reserves the right to monitor company systems, devices, accounts, logs, communications and network activity where lawful, proportionate and necessary for security, compliance, investigations, operations, audit, legal obligations or protection of Kovon's rights and data.

Monitoring will be conducted in accordance with applicable law and should be limited to legitimate business purposes. Users should not expect unrestricted privacy when using Kovon systems or accounts.

18. Vendor, Client and Third-Party Access

Third-party access to Kovon systems or data must be approved, documented, limited by purpose and removed when no longer needed. Vendors must follow confidentiality, privacy, security and incident-notification obligations appropriate to the data and systems accessed.

Vendor integrations, background verification platforms, payroll tools, cloud systems, CRM tools, AI services and website/app admin tools must be reviewed for security risk before production use where feasible.

19. Training and Acknowledgement

Covered users must complete security awareness training appropriate to their role. Users with access to candidate data, HR data, payroll, code repositories, production systems, cloud systems or admin panels may receive additional role-based training.

Acknowledgement of this policy is mandatory for covered users with access to Kovon systems, data, code, devices or accounts.

20. Exceptions, Breaches and Review

Exceptions to this policy must be approved under the Corporate Policy Governance Framework. No exception may permit unlawful activity, credential sharing, concealment of an incident, unauthorised data transfer, intentional security bypass or use of unapproved public AI tools with protected Kovon data.

Breaches of this policy may result in access restriction, retraining, disciplinary action, contract action, vendor action, termination, reporting to authorities or legal proceedings depending on severity and applicable law.

This policy will be reviewed annually by the CTO / Security Owner with CEO, IT Admin, Engineering Head and Head of People input and submitted to the Board of Directors for approval of material changes.

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: Minimum Security Checklist

30. Use MFA on email, HRMS, ATS, CRM, cloud, code repositories and admin tools.
31. Do not share credentials or reuse business passwords.
32. Use approved systems for Kovon data.
33. Do not share high-risk data over WhatsApp or personal messaging.
34. Do not enter Kovon protected data into unapproved public AI tools.
35. Lock screens and secure devices, especially during remote work.
36. Report phishing, lost devices, credential compromise, data leaks and system breaches immediately.
37. Remove access promptly when roles change or engagement ends.
38. Use branch protection, code review and secrets management for engineering work.
39. Ask the CTO / Security Owner before using a new tool with Kovon data.

Appendix B: Acknowledgement

I acknowledge that I have received or been given access to Kovon's Information Security and Acceptable Use Policy. I understand that I am expected to protect Kovon systems, data, credentials, devices and code; use approved tools; follow access and BYOD rules; and report suspected security incidents promptly.

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