FAIR ETHICS POLICY

HIKAL LIMITED

Revision Number:
01

Version Control

Date	Revision Number	Comment
01st April 2025	00	Initial Release
01st September 2025	1.0	Updates in Section 4.3 "Anti Corruption & Bribery"- 'require pre-approval, documentation, and periodic review of gifts, hospitality, donations, sponsorships, and charitable contributions'. Section 5.5- 'cover 100% of employees through conflict-of-interest awareness training'

Next Review Date: 01st September 2026

Sameer Hiremath

Approved by:

Sameer Hiremath,
Vice Chairman & Managing Director

Table of Contents

1. Preamble

Hikal Ltd. (Group) is committed to conducting all business activities with the highest standards of integrity, fairness, transparency, and accountability. Ethical conduct is fundamental to the Company's long-term value creation, stakeholder trust, and regulatory compliance. This Fair Ethics Policy establishes the principles and expectations governing the behaviour of all employees, contractors, partners, suppliers, and other stakeholders associated with Hikal Ltd. It ensures that all business decisions are made in a manner that is honest, transparent, and aligned with applicable laws, regulations, and industry best practices.

2. Applicability

This Fair Ethics Policy applies to all employees, stakeholders, contractors, partners, customers, contract workers, and any individuals representing the Hikal Limited Group. It is applicable to all manufacturing units, operational facilities, branch offices, registered locations, warehouses, and any other premises owned, leased, or managed by the Hikal Limited Group, as listed below:

Sr. No.	Name	Function	Address
1	Hikal Limited	Registered Office	717 / 718, Maker Chamber V, Nariman Point, Mumbai – 400021
2		Corporate Office	Great Eastern Chambers, Sector 11, CBD Belapur, Navi Mumbai - 400 614, India.
3		Manufacturing Plant	T-21, MIDC. Industrial Area, Taloja - 410 208, District Raigad, Maharashtra, India.
4			A-18, MIDC Industrial Area, Mahad - 402 309, District Raigad, Maharashtra, India.
5			629 / 630-B, GIDC Estate, Panoli -394 116, District Bharuch, Gujarat, India.
6			JIGANI UNIT I: 82/A, KIADB Industrial Area, Jigani, Anekal Taluk, Bangalore – 560 105, India.
7			JIGANI UNIT II: 28, KIADB Industrial Area, Jigani, Anekal Taluk, Bangalore – 560 105, India.
8		Research and Technology (R&T) Centres	Plot No. 3A & 3B, 2nd Phase, International Biotech Park, Hinjewadi, Pune - 411 057, India.
9		Marketing office	3rd floor, Grey Rock, No.10, 24th Main, J.P. Nagar, 2nd Phase, Bangalore - 560 078, India.

10		Office	Kyodo Bldg. 503, 1-18 Kanda Sudacho, Chiyoda-ku, Tokyo 101-0041, Japan.
11			Marketing Office, USA
12			Marketing Office, Europe

3. Focus Areas

- Integrity and ethical conduct in all business activities
- Zero tolerance towards bribery, corruption, fraud, and unethical practices
- Identification, disclosure, and management of conflicts of interest
- Promotion of fair competition and responsible business practices
- Respect for human rights, dignity, diversity, and non-discrimination
- Protection of confidential, proprietary, and personal information
- Responsible and appropriate use of company assets and resources
- Transparent reporting of ethical concerns through established mechanisms

4. Hikal's Ethical Commitments

4.1 Information Security and Management

→ We commit to maintaining an enterprise-wide Information Security Management System (ISMS) with clearly defined roles, responsibilities, and access controls for all critical information assets.

→ We will implement information based on sensitivity and apply role-based access, multi-factor authentication, and encryption for confidential and personal data.

→ We will conduct periodic vulnerability assessments, penetration testing, and system access reviews to identify and remediate information security risks.

→ We commit to maintaining documented incident response and data breach management procedures, including timely internal escalation and regulatory reporting where required.

→ We will provide mandatory information security and cyber awareness training to all employees, with enhanced training for personnel handling sensitive or regulated data.

4.2 Data Manipulation

→ We aim to see that all financial, operational, regulatory, and ESG data is recorded, processed, and reported accurately and in a timely manner.

- → We prohibit unauthorized alteration, suppression, or misrepresentation of data, including manipulation of laboratory results, quality records, financial statements, or sustainability disclosures.
- → We endeavor to implement segregation of duties, maker-checker controls, and system-based validations for data creation, modification, and approval processes.
- → We will ensure to conduct periodic internal audits and management reviews of critical data sets and reporting processes.
- → We will investigate all reported instances of suspected data manipulation and take corrective and disciplinary action in line with company policies and applicable laws.

4.3 Anti Corruption & Bribery

- → We commit to a zero-tolerance approach towards bribery, corruption, facilitation payments, kickbacks, or improper benefits in any form, whether direct or indirect.
- → We prohibit offering, giving, soliciting, or accepting bribes, including through third parties such as agents, consultants, distributors, or intermediaries.
- → We will require pre-approval, documentation, and periodic review of gifts, hospitality, donations, sponsorships, and charitable contributions.
- → We will conduct corruption risk assessments and due diligence for high-risk third parties, geographies, and transactions.
- → We will ensure mandatory anti corruption training for all employees in procurement, sales, finance, regulatory, and leadership roles.

4.4 Anti Money Laundering

- → We commit to strict compliance with applicable anti money laundering (AML) laws and regulations, ensuring due diligence is applied to all relevant financial transactions and business relationships.
- → We will implement systematic screening and verification of customers, business partners, and transactions to detect and prevent money laundering, terrorist financing, or other illicit activities.
- → We commit to providing periodic AML training to employees in finance, procurement, sales, and other relevant functions to enhance awareness of risk indicators, reporting obligations, and due diligence procedures.
- → We will ensure comprehensive KYC checks are completed and documented prior to onboarding third parties, entering into contracts, or executing high-value or high-risk transactions.
- → We will maintain accurate, secure, and retrievable records of financial transactions, due diligence documentation, and third-party engagements in line with AML requirements and audit and regulatory expectations.

4.5 Conflict of Interest

→ We maintain zero tolerance for non-disclosure, concealment, or misuse of position arising from conflicts of interest, and will take disciplinary action in line with Company policies and applicable laws
→ We commit to requiring employees to proactively disclose any personal, financial, or familial interests that may influence, or appear to influence, professional judgment or business decisions.
→ We will provide clear procedures and guidance to managers for identifying, assessing, and mitigating actual, potential, or perceived conflicts of interest.
→ We aim to strengthen awareness through periodic training and communication on conflict-of-interest scenarios, ethical decision-making, and reporting responsibilities across all functions.
→ We commit to ensuring that all disclosed conflicts of interest are appropriately reviewed, managed, and resolved in a transparent manner, reinforcing a strong and consistent compliance culture.

4.6 Prevention of Fraud

→ We aim to establish and maintain robust internal controls and clearly defined approval procedures to proactively detect, deter, and prevent fraudulent activities across all operations and financial processes.
→ We will strengthen internal control frameworks to ensure effective identification, timely reporting, and prevention of fraud across all business functions.
→ Our aim is to foster a transparent and ethical culture that encourages employees and stakeholders to report suspected or observed fraudulent activities without fear of retaliation.
→ We will ensure comprehensive, structured, and role-based fraud prevention training is provided to employees at regular intervals to enhance awareness, reinforce ethical conduct, and build capability to identify and respond to fraud risks.
→ We will ensure continuous enhancement in employee knowledge, skills, and compliance through ongoing training programs aligned with organizational policies, ethical standards, and applicable regulatory requirements.

5. Targets

5.1 Information Security and Management

→ We aim to implement formal information security controls across 100% of critical IT systems by FY 2027-28.
→ We aim to achieve that 100% of employees receive annual training on information security and data privacy by 2027-28.

→ We maintain encryption and access controls 100% on all critical systems and devices across the organization by 2027-28.
→ We continuously respond to reported 100% data-breach incidents within 12 hours by 2027-28.
→ We aim to maintain zero confirmed cases of information security breaches, unauthorized access, or data loss each year.

5.2 Data Manipulation

→ We aim to establish documented data integrity and approval controls for 100% of critical data and reporting processes by FY 2026–27.
→ We aim to cover 100% of relevant employees through mandatory data integrity and ethical reporting training by FY 2026–27.
→ We strive to maintain zero confirmed cases of intentional data manipulation.

5.3 Anti Corruption & Bribery

→ We aim to train all the employees on ethics and anti corruption training, fraud, insider trading, and anti competitive behaviour annually, with enhanced training provided to high-risk functions such as sales, procurement, and operations by 2027-28.
→ We aim to achieve 100% of contracts with agents, distributors, and consultants including clear anti bribery and corruption clauses by 2027-28.
→ We aim to maintain zero confirmed cases of bribery, facilitation payments, fraud, insider trading, anti competitive behaviour or improper influence each year.
→ We aim to conduct anti corruption due diligence for all HR third-party engagements by FY 2027–28.

5.4 Anti Money Laundering

→ We aim to implement AML, fraud, insider trading, anti competitive behaviour screening and monitoring mechanisms for 100% of applicable customers, vendors, and intermediaries by FY 2027–28 sustaining the performance achieved in previous years.
→ We aim to maintain 100% of payments through traceable banking channels and report all suspicious transactions in line with regulatory requirements by 2027-28, sustaining the performance achieved in previous years.
→ We strive to cover 100% of employees through AML awareness and compliance training by FY 2027–28.
→ We aim to conduct periodic AML risk assessments across all applicable operations by FY 2027–28.
→ We seek to maintain zero confirmed cases of money laundering or regulatory non-compliance by FY 2027–28.

5.5 Conflict of Interest

→ We aim to obtain annual conflict of interest declarations from all relevant employees and key management by FY 2027–28, covering areas such as personnel on nepotism, financial self-dealing, accepting improper gifts, outside employment, political affiliations or misuse of confidential information.

→ We strive to ensure that all the identified conflict of interest cases are documented, reviewed, and resolved through defined processes by FY 2027–28.

→ We aim to cover all the employees through conflict-of-interest awareness training by FY 2027–28.

→ We aim to maintain zero cases of conflict-of-interest cases per year by FY 2027-28.

5.6 Prevention of Fraud

→ We aim to ensure fraud risk assessments and control mechanisms across high-risk business areas and financial processes by FY 2027–28.

→ We strive to cover all the employees through mandatory trainings on topics including but not limited to fraud, insider trading, anti competitive behaviour prevention, and awareness by FY 2027–28.

→ We aim to conduct regular internal audits and ensure that financial and operational records are reviewed according to the internal control schedule by 2027-28.

→ We are committed to investigating 100% reported fraud allegations within scheduled time and implementing corrective actions, where required.

→ We aim to maintain zero confirmed fraud incidents per year.

6. Consequences of Policy Violations

- Violations of the Fair Ethics Policy may result in disciplinary action, up to and including termination of employment or contract.
- Serious breaches, including bribery, corruption, fraud, data manipulation, or conflicts of interest, may result in legal action under applicable laws and regulations.
- Non-compliance with mandatory training or awareness programs may lead to restrictions on system access, project participation, or role responsibilities.
- Unauthorized disclosure, misuse, or loss of confidential information or company assets may result in financial recovery, disciplinary action, or legal proceedings.
- Acts of retaliation against individuals reporting concerns in good faith will result in strict disciplinary measures, including termination, and potential legal consequences.

- All violations will be investigated promptly, fairly, and confidentially, with actions proportionate to the severity, impact, and recurrence of the breach.
- Continuous or repeated violations may affect career progression, performance appraisal, and eligibility for internal opportunities.
- Hikal Ltd. reserves the right to take any additional action deemed necessary to protect the company, its stakeholders, and compliance with laws and regulations.

7. Employee Guidelines

Employees of Hikal Ltd. are expected to uphold the highest standards of ethical conduct and comply with all aspects of the Fair Ethics Policy. The following guidelines provide practical instructions for employees to follow:

7.1 Integrity and Ethical Conduct

- Always act with honesty, fairness, and transparency in all business dealings.
- Avoid any behaviour that could damage Hikal Ltd.'s reputation or stakeholder trust.
- Report any suspected unethical behaviour, misconduct, or breaches of company policy immediately.
    - **Do:** Report all work activities truthfully and maintain transparency in communications.
    - **Don't:** Hide errors, manipulate facts, or misrepresent information to improve personal or departmental outcomes.

7.2 Compliance with Laws and Regulations

- Follow all applicable laws, regulations, and internal company policies in every action and decision.
    - **Do:** Stay informed about relevant regulations and seek guidance when unsure.
    - **Don't:** Ignore legal requirements or bypass company policies to achieve business targets.

7.3 Bribery and Corruption

- Never offer, give, solicit, or accept bribes, facilitation payments, kickbacks, or any form of improper benefit.
- Ensure all gifts, hospitality, donations, or sponsorships comply with company approval procedures.
- Conduct due diligence on all third parties to avoid involvement in corrupt practices.

- **Do:** Obtain approval for any gift, hospitality, or donation as per policy.
- **Don't:** Give or accept money, favours, or gifts to influence decisions.

7.4 Conflict of Interest

- Disclose any personal, financial, or familial interests that may influence, or appear to influence, business decisions.
- Recuse yourself from decisions where a conflict of interest exists until the matter is reviewed and resolved.
- Update conflict-of-interest declarations annually or whenever new conflicts arise.

  - **Do:** Notify your manager if you have a family member working for a vendor.
  - **Don't:** Make decisions benefiting yourself or family without disclosure.

7.5 Anti Money Laundering (AML)

- Follow all AML procedures when dealing with customers, vendors, or third parties.
- Report any suspicious transactions or activities immediately to the Compliance team.
- Ensure accurate documentation and retention of all financial and contractual records.

  - **Do:** Verify the identity of new vendors and follow KYC checks.
  - **Don't:** Ignore unusual payment patterns or bypass due diligence procedures.

7.6 Data Integrity and Reporting

- Ensure that all financial, operational, laboratory, and ESG data is accurate, complete, and timely.
- Never manipulate, falsify, or suppress data for personal or professional gain.
- Follow all internal approval and maker-checker processes for data creation, modification, and reporting.

  - **Do:** Enter data carefully and double-check before submitting reports.
  - **Don't:** Falsify, alter, or suppress data to meet targets or deadlines.

7.7 Information Security

- Protect company information and systems by following ISMS policies, including password controls, multi-factor authentication, and encryption.
- Report any suspected or actual information security incidents immediately.
- Use company IT resources responsibly and only for authorized purposes.

- **Do:** Lock your workstation, use strong passwords, and report phishing emails.
- **Don't:** Share passwords, leave sensitive files exposed, or use unauthorized devices.

7.8 Fraud Prevention

- Be vigilant and proactive in identifying and reporting any suspected fraudulent activity.
- Participate in mandatory fraud prevention training programs.
- Support internal investigations and audits by providing accurate information.

  - **Do:** Report any suspicious behaviour or transactions to the Compliance team.
  - **Don't:** Participate in or ignore fraudulent schemes, misappropriation, or misuse of company assets.

7.9 Reporting Violations

- Use designated reporting channels to report concerns, misconduct, or violations of this Policy. Please refer to section 11 of this Policy for the designated channels.
- Reports made in good faith will be treated confidentially, and employees will be protected from retaliation.
  - **Do:** Use the whistleblower hotline, email, or reporting portal to raise concerns.
  - **Don't:** Ignore violations, cover up incidents, or retaliate against reporters.

7.10 Training and Awareness

- Complete all mandatory training programs on ethics, anti corruption, AML, fraud, insider trading, anti competitive behaviour, conflict-of-interest, and information security.
- Seek guidance from managers or the Compliance team when in doubt about ethical or policy matters.

  - **Do:** Attend scheduled trainings, refresher sessions, and apply learnings to daily work.
  - **Don't:** Skip mandatory courses, ignore updates, or fail to apply policy guidance in work activities.

7.11 Respect and Fair Treatment

- Treat all colleagues, partners, and stakeholders with respect, dignity, and fairness, promoting diversity and inclusion.
  - **Do:** Listen actively, recognize differences, and maintain professionalism.

- **Don't:** Harass, discriminate, or make biased decisions based on gender, race, religion, or background.

8. Governance & Responsibility

8.1 Managing Director

→ Provide strategic oversight and ensure that the Fair Ethics Policy aligns with corporate governance standards and regulatory requirements.
→ Review significant ethical breaches, corruption cases, fraud incidents, conflicts of interest, and data manipulation cases, and report to the Board, if required
→ Allocate necessary resources for ethics programs, awareness campaigns, and compliance monitoring.
→ Promote a culture of integrity, transparency, and accountability across the organization.

8.2 President HR

→ Ensure the effective implementation of the Fair Ethics Policy across all functions and business units.
→ Lead by example and reinforce a zero-tolerance approach towards unethical practices, bribery, corruption, and fraud.
→ Regularly review organizational ethical performance and report to the Managing Director.
→ Drive integration of ethics and compliance considerations into strategic and operational decisions.

8.3 Executive Director ESG

→ Track ethics KPIs and disclosures (incidents, training, declarations)
→ Strengthen whistleblower and grievance mechanisms.
→ Promote an ethical culture and accountability across the organization.

8.4 Chief Financial Officer

→ Ensure accurate, transparent, and timely financial reporting in line with regulatory requirements.
→ Implement internal controls to prevent financial fraud, data manipulation, and money laundering.

8.5 Head Sustainability & Corporate EHS

→ Monitor ESG performance related to employee rights and fair ethics.
→ Ensure participation in strengthening of monitoring systems, audits, inspections, and corrective actions.
→ Integrate ethics into risk assessments and supplier due diligence.
→ Drive training and awareness across employees.
→ Support audits and corrective actions (e.g., SMETA, EcoVadis)

8.6 Head IT

→ Implement and maintain the Information Security Management System (ISMS) for all critical systems.
→ Ensure proper access controls, multi-factor authentication, encryption, and regular security audits.
→ Conduct periodic vulnerability assessments, penetration testing, and data breach simulations.
→ Coordinate mandatory cybersecurity and data privacy awareness training for employees.

8.7 Human Resources (HR)

→ Integrate ethical principles and compliance requirements into hiring, onboarding, and performance management processes.
→ Facilitate training programs on ethics, anti corruption, conflict of interest, and fraud prevention.
→ Manage whistleblower and grievance mechanisms, ensuring protection against retaliation.
→ Maintain records of employee disclosures, conflict-of-interest declarations, and training completion.

8.8 Corporate HR

→ Develop, maintain, and update the Fair Ethics Policy and associated procedures.
→ Oversee implementation of anti corruption, anti money laundering (AML), fraud prevention, conflict of interest, and information security controls by the IT Department.
→ Ensure that all employees, contractors, and third parties receive mandatory ethics, AML, anti bribery, and fraud prevention training.

8.9 All Employees, Contractors, and Third Parties

→ Adhere to the Fair Ethics Policy and related procedures in all business activities.
→ Disclose any actual, potential, or perceived conflicts of interest in a timely manner.
→ Report suspected violations of ethics, fraud, data manipulation, bribery, or corruption through established channels.
→ Protect confidential and proprietary information and use company resources responsibly.
→ Follow the employee guidelines.
→ Participate in mandatory ethics, compliance, AML, anti corruption, and fraud awareness training.

8.10 Ethics Committee

- → Provide independent oversight into the implementation of the Fair Ethics Policy across the organization.
- → Review reported ethical breaches, whistleblower complaints, and investigation outcomes.
- → Ensure fair, unbiased, and timely resolution of ethics-related cases.
- → Recommend disciplinary actions and corrective measures in line with company policies.
- → Monitor effectiveness of whistleblower and grievance mechanisms.
- → Review trends in ethics incidents and systemic risks and suggest preventive actions.
- → Ensure consistency in decision-making across cases and business units.
- → Oversee closure of high-risk or sensitive cases, including escalation where required.
- → Guide improvements in ethics governance, controls, and processes.
- → Report periodically to senior management/Board on ethics performance and key issues.

9. Reporting & Monitoring

Employees and stakeholders must promptly report any suspected violations, misconduct, or ethical concerns through designated channels, including the whistleblower hotline, email, or reporting portal. All reports will be treated confidentially and investigated impartially. The Compliance team, Internal Audit, and management will monitor adherence to this Policy, track incidents, implement corrective actions, and ensure timely reporting to leadership and regulatory authorities as required. Please refer to section 11 of this Policy for the designated channels.

10. Continuous Improvement

Hikal Ltd. is committed to continuously enhancing its ethical standards, compliance frameworks, and risk management practices. Policies, procedures, and training programs will be periodically reviewed and updated based on audits, feedback, regulatory changes, and industry best practices. Employees are encouraged to provide suggestions for improvement. Lessons learned from investigations, incidents, and audits will be applied to strengthen controls, promote ethical behaviour, and drive sustainable and responsible business growth.

11. Grievance Mechanism and Contact Information

In case of any grievance, questions or concerns with regards to the Policy, please reach out to us through the following channels:

External Stakeholders	community_grievance@hikal.com or call at 022-62770299
Internal Stakeholders	employee_grievance@hikal.com Alternatively, grievances may be submitted anonymously by depositing them in the designated complaint/grievance boxes available at all sites

All concerns will be handled with appropriate confidentiality and in accordance with the Hikal's grievance redressal procedures.

12. Policy alignments with SDGs

13. Policy Review Mechanism

Hikal Ltd. will conduct periodic reviews of the Fair Ethics Policy annually or as required to ensure its continued relevance, effectiveness, and alignment with regulatory requirements and industry best practices. Reviews will include assessment of policy implementation, compliance metrics, training effectiveness, incident reports, and feedback from employees and stakeholders. Updates will be approved by senior management and communicated to all employees to reinforce a culture of integrity, accountability, and continuous improvement.

14. Disclaimer

This policy is a proprietary to the Hikal limited. Unauthorised use, replication, or distribution of this document or its contents, in whole or in part, is strictly prohibited without prior written consent. The information contained herein is subject to continuous review and updates, and may be modified to reflect evolving business conditions, regulatory requirements or operational strategies. Hikal limited assumes no responsibility or liability for unauthorised reliance on or misinterpretation of this policy.