

AILOGIX SYSTEMS PRIVATE LIMITED

Code of Conduct & Ethics Policy

Document Control Number: ALGX-POL-ETH-001

Effective Date: June 08, 2026

Applicability: All Board Members, Executive Leadership, Permanent & Temporary Employees, Software Trainers, Instructional Staff, Consultants, Contractors, and Interns across all offices and training facilities of AILOGIX SYSTEMS PRIVATE LIMITED.

1. Purpose & Core Values

AILOGIX SYSTEMS PRIVATE LIMITED ("AILOGIX" or "the Company") is committed to delivering high-quality software development, IT services, and industry-aligned software training with the highest standards of professional and ethical integrity.

Our foundational principles are:

- **Integrity & Transparency:** Doing the right thing in code quality, client dealings, and trainee evaluations.
- **Excellence in Pedagogy & Engineering:** Delivering real-world software expertise through authentic training and engineering practices.
- **Respect & Fairness:** Maintaining an inclusive, harassment-free environment for employees, clients, and students alike.
- **Data Privacy & Security:** Safeguarding client proprietary software, student personal records, and intellectual property.

2. Workplace Culture & Employee Welfare

2.1 Prevention of Sexual Harassment (POSH)

AILOGIX enforces a strict **Zero-Tolerance Policy** toward sexual harassment in accordance with the *Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013* (India).

- Harassment of any kind—verbal, non-verbal, physical, or digital—directed toward colleagues, client personnel, or trainees is prohibited.
- The Internal Complaints Committee (ICC) handles all POSH grievances confidentially and within statutory timelines.

2.2 Diversity, Non-Discrimination & Equal Opportunity

- Employment, promotions, trainer assignments, and student admissions are made solely on merit, skill, and performance.
- Discrimination based on gender, race, caste, religion, age, sexual orientation, disability, or marital status is strictly prohibited.

3. Ethics in Software Services Delivery

When representing AILogix in software engineering, IT consulting, custom application development, or system integration:

3.1 Code Quality & Software Integrity

- **No Unsanctioned Code / Malware:** Software engineers must not intentionally introduce backdoors, malicious code, or unauthorized telemetry into client deliverables.
- **Licensing & Open Source (OSS) Compliance:** Software developers must follow licensing protocols. Copying open-source code with restrictive licenses (e.g., GPL) into proprietary client software without written approval is strictly prohibited.

3.2 Client Confidentiality & Non-Disclosure (NDA)

- Employees must safeguard all client intellectual property, source code, database credentials, architecture diagrams, and business strategies.
- Client data must never be used for personal projects, external freelancing, or training materials without explicit, written authorization from the client and AILogix management.

4. Ethics in Software Training & Academic Operations

As an institution delivering software training, AILogix holds its instructional and administrative staff to elevated standards of academic and professional responsibility.

4.1 Trainer Professionalism & Student Interactions

- **Objective Evaluation:** Student assessments, project evaluations, certification scores, and feedback must be conducted impartially, free from favoritism or personal bias.
- **Boundaries:** Trainers and instructors must maintain professional boundaries with trainees and students. Exploiting student-instructor dynamics for financial, personal, or unauthorized gain is grounds for immediate termination.

4.2 Academic Integrity & Anti-Plagiarism

- Course materials, code templates, and curriculum produced by AILogix must respect copyright laws. Unattributed copying of third-party educational content is prohibited.

- Trainees must be taught and held to professional standards of code authorship, fair practice, and authentic project submissions.

5. Conflicts of Interest & Business Integrity

5.1 Moonlighting & External Engagement

- Full-time employees and trainers of AILogIX are prohibited from undertaking secondary software development, external corporate training, freelancing, or consulting for direct competitors without prior written approval from Human Resources and Management.

5.2 Anti-Bribery & Corruption

- AILogIX maintains zero tolerance for bribery, kickbacks, or unlawful inducements under the *Prevention of Corruption Act* or international anti-corruption standards.
- Neither employees nor training staff may offer or receive gifts, cash, or favors exceeding ₹2,500 (or equivalent) to/from clients, vendors, government representatives, or students.

6. Information Security & Data Protection

Domain	Mandatory Guideline
Data Protection	Full compliance with the <i>Digital Personal Data Protection (DPDP) Act</i> (India) and relevant global data privacy regulations.
Access Control	Employees and trainers must use Multi-Factor Authentication (MFA) on all company-issued accounts, GitHub organizations, and LMS portals.
System Security	Production database keys, client server credentials, and student personal identifiable information (PII) must never be committed to public code repositories (e.g., public GitHub/GitLab).
Device Usage	Company-issued hardware and network access must be used for official work and training purposes only.

7. Reporting & Whistleblower Mechanism

AILOGIX encourages a culture where employees, contract staff, and trainees feel safe raising ethical concerns.

How to Report Misconduct

- **Email Escalation:** Submit reports directly to hr@ailogixit.com
- **Anonymous Whistleblower Hotline:** Accessible via the internal portal for reporting financial irregularities, data breaches, or systemic misconduct.

Protection Against Retaliation: AILOGIX guarantees that no individual making a report in good faith will suffer retaliation, demotion, termination, or academic discrimination.

8. Violations & Disciplinary Actions

Failure to adhere to this Code of Conduct will result in disciplinary proceedings proportional to the severity of the offense:

1. **Minor Infractions:** Verbal warning, mandatory ethics or security retraining, and official documentation.
2. **Moderate Infractions:** Written reprimand, suspension, withholding of performance incentives, or reassignment.
3. **Severe Violations:** Immediate termination of employment or contract, forfeiture of certification rights (for trainees), and potential legal action under applicable Indian civil/criminal statutes.