Employee Handbook & Operational Policies

Version: 4.2
Effective Date: January 01, 2026

1. INTRODUCTION
Welcome to Intra. We are pioneering the future of autonomous systems through Agentic AI. This handbook outlines the policies and procedures that govern our operations. As an employee of Intra, you are expected to uphold the highest standards of integrity, professionalism, and technical excellence. Our mission is to build AI agents that are safe, reliable, and aligned with human intent.

2. CODE OF CONDUCT
2.1 Professionalism
Employees are expected to maintain a professional demeanor at all times. Respect for colleagues, clients, and partners is paramount. Harassment or discrimination of any form is strictly prohibited and will result in immediate disciplinary action.

2.2 Confidentiality
Given the sensitive nature of our proprietary algorithms and client data, confidentiality is critical. Employees must not disclose trade secrets, source code, or model weights to unauthorized parties. All work products created during your employment are the sole property of Intra.

3. WORKPLACE OPERATIONS

3.1 Standard Business Hours
Our core operating hours are 10:00 AM to 4:00 PM (Local Time). However, we operate on a results-oriented culture. Employees are free to manage their schedules outside of core hours, provided that deadlines are met and meetings are attended.

3.2 Remote Work Policy
Intra supports a hybrid work environment. Employees may work remotely up to 3 days per week. When working remotely, employees must ensure they have a stable internet connection and a private workspace to maintain data security. Video backgrounds during external calls should be professional.

4. INFORMATION SECURITY & DATA PRIVACY

4.1 Device Management
All company-issued laptops must be encrypted and protected by the corporate VPN. Personal devices may not be used to access the production database or the Model Registry.

4.2 Access Control
Access to production environments is granted on the Principle of Least Privilege. Requests for elevated permissions must be approved by the Security Operations Center (SOC). Multi-Factor Authentication (MFA) is mandatory for all internal systems.

4.3 Data Handling
Customer data must never be used for model training without explicit consent and anonymization. Employees must strictly adhere to GDPR and CCPA compliance guidelines when handling user datasets.

5. ACCEPTABLE USE OF AI RESOURCES

5.1 Internal GPU Usage
Company GPU clusters are prioritized for production inference and scheduled training jobs. Exploratory research requiring significant compute must be scheduled via the Resource Manager.

5.2 Third-Party AI Tools
The use of external generative AI tools (e.g., public ChatGPT, Midjourney) for proprietary code generation or business strategy is restricted. Employees must use the internal 'Intra-GPT' instance which ensures data is not sent to third-party model trainers.

6. LEAVE AND TIME OFF

6.1 Annual Leave
Full-time employees are entitled to 20 days of paid annual leave. Leave requests should be submitted at least 2 weeks in advance via the HR portal.

6.2 Sick Leave
Employees are allotted 10 days of sick leave per year. For absences exceeding 3 consecutive days, a medical certificate may be required.

7. DISCIPLINARY PROCEDURES
Violations of these policies will be addressed through a graduated disciplinary process, ranging from verbal warnings to termination of employment, depending on the severity of the infraction.

_____
Employee Signature

_____
Date