

# Corporate Policy Manual

This handbook outlines organizational policies governing ethics, conduct, safety, attendance, and compliance. All employees are required to understand these rules and acknowledge them annually through the HR portal.

The policies apply to full-time, part-time, contractual, and remote employees unless otherwise specified in writing. Violations may lead to disciplinary action including warnings, suspension, or termination depending on severity.

## Code of Conduct

Employees must act professionally and respectfully toward colleagues, customers, vendors, and partners. Harassment, discrimination, bullying, or intimidation of any kind is strictly prohibited.

Conflicts of interest must be disclosed to management. Accepting gifts or favors that could influence business decisions requires prior written approval from the compliance department.

## Leave and Attendance Policy

Employees are entitled to twenty days of paid annual leave per calendar year in addition to official public holidays. Unused leave may be carried forward subject to company limits and local labor laws.

Sick leave may be taken for illness or medical appointments and should be reported to the manager before the start of the workday whenever possible. Medical certificates may be requested for extended absences.

Planned vacations must be submitted through the HR management system at least two weeks in advance and approved by the reporting manager.

## **Working Hours and Remote Work**

Standard working hours are from 9:00 AM to 6:00 PM, Monday through Friday, with one hour for lunch. Flexible schedules may be approved depending on team requirements.

Employees working remotely must maintain reliable internet connectivity, protect company equipment, and follow the same productivity and confidentiality standards as on-site staff.

## **Information Security Policy**

Passwords must be at least twelve characters long and include a combination of uppercase letters, lowercase letters, numbers, and special symbols. Passwords must be changed every ninety days.

Company systems may only be accessed using authorized devices and approved software. Employees must immediately report any suspected security incident or phishing attempt to the IT department.

## **Data Protection and Privacy**

Confidential information must be encrypted when stored or transmitted. Access is restricted to authorized personnel based on job responsibilities.

Personal data of employees and customers must be handled in accordance with applicable privacy laws and company data protection standards.

## **Disciplinary Process**

Minor violations may result in verbal or written warnings, while repeated or serious misconduct can lead to suspension or termination of employment.

Employees have the right to appeal disciplinary decisions through the grievance redressal process outlined in the employee handbook.