At InfoFlow AI, our mission is to foster a transparent, secure, and inclusive workplace where technology and people thrive together. To achieve operational excellence and employee satisfaction, clear guidelines must be in place for each department. This document outlines detailed protocols and behavioral expectations for IT personnel and Human Resources (HR) professionals.

💻 IT Employee Guidelines

The IT department is the backbone of InfoFlow AI's digital infrastructure. To ensure security, efficiency, and compliance with industry standards, all IT employees must adhere to the following rules:

1. Cybersecurity and Data Protection

- All IT staff must follow InfoFlow AI's cybersecurity protocols, including the use of firewalls, antivirus software, and secure connections.
- Employees must never share login credentials, passwords, or encryption keys.
- Multifactor authentication (MFA) must be enabled on all administrative accounts.
- Regularly monitor systems for intrusion, unauthorized access, and data breaches.

2. Software Usage and Licenses

- Only authorized and licensed software may be installed or used on company systems.
- IT employees must keep an inventory of installed software and ensure compliance with licensing agreements.
- Any request for new software installation must be approved through the internal IT service portal.

3. System Access and Permissions

- Grant system access on a “least privilege” basis, meaning employees get only the access required to perform their roles.
- Ensure timely revocation of system access for departing employees.
- Maintain audit trails of system access, login times, and data operations for security reviews.

4. Incident Reporting and Troubleshooting

- All IT issues must be reported via the ticketing system and resolved according to defined SLAs (Service Level Agreements).
- Security incidents, data leaks, or suspicious system behavior must be escalated immediately to the CISO or Security Head.
- Maintain logs of incidents and solutions to build a knowledge base.

5. Device Management and Maintenance

- Ensure timely updates and maintenance of laptops, servers, routers, and all digital assets.
- Enforce device encryption on all company-issued machines.
- Regular backups of critical systems and cloud storage must be verified weekly.

6. Workplace Conduct and Communication

- Maintain professionalism when engaging with non-technical teams. Avoid jargon.
- Communicate outages, downtime, or maintenance in advance to relevant stakeholders.
- Encourage feedback from end users to improve IT support and services.

7. Remote Work Policy for IT Staff

- Use VPNs to access company resources remotely.
- Secure personal devices used for remote access with antivirus software and endpoint protection.
- Follow the same compliance and privacy standards as in-office work.

👥 HR Employee Guidelines

The Human Resources team plays a vital role in shaping the culture and compliance standards of InfoFlow AI. The following guidelines ensure ethical conduct, legal compliance, and the emotional well-being of our workforce.

1. Recruitment and Onboarding

- Ensure that all job postings are inclusive and adhere to equal employment opportunity (EEO) guidelines.
- Conduct background checks where necessary in compliance with local laws.

- Provide a structured onboarding process that includes IT orientation, policy training, and role-specific knowledge.

2. Employee Data Privacy

- HR must ensure confidentiality of employee records such as medical history, salary, personal identification, and disciplinary actions.
- Avoid storing sensitive employee information in unprotected or publicly accessible systems.
- Access to employee data should be role-restricted and monitored.

3. Performance and Appraisal Management

- Ensure timely performance evaluations with structured feedback.
- Train managers on fair appraisal techniques to avoid bias or favoritism.
- Use measurable KPIs and SMART goals in evaluation forms.

4. Conflict Resolution and Grievance Redressal

- Provide employees with multiple safe channels to report harassment, discrimination, or workplace disputes.
- All complaints must be investigated confidentially and resolved within a defined timeframe.
- Retaliation against employees raising valid concerns is strictly prohibited.

5. Compliance and Legal Adherence

- Stay updated on labor laws, EEO requirements, and health & safety regulations.
- Ensure timely compliance filings for PF, ESI, tax declarations, maternity/paternity leaves, etc.
- Conduct regular audits to verify HR policy adherence.

6. Training and Development

- Organize mandatory sessions on workplace ethics, diversity and inclusion, and cybersecurity awareness.
- Encourage professional growth through technical certifications, soft skill workshops, and learning stipends.
- Maintain records of completed training and certifications.

7. Exit Management

- Conduct structured exit interviews to gather insights and feedback.
- Ensure all company assets (laptops, IDs, access cards) are collected on or before the last working day.
- Collaborate with IT to ensure revocation of system access upon employee termination.

🗃️ Shared Guidelines for IT & HR Collaboration

Collaboration between HR and IT is essential for enforcing policies and ensuring smooth operations:

- **Onboarding Coordination:** HR must inform IT of new joiners at least 3 business days in advance for device and access provisioning.
- **Offboarding Sync:** On an employee's last working day, HR and IT must coordinate to revoke access, collect devices, and update internal systems.
- **Policy Updates:** Any updates to HR policies impacting device usage, remote work, or data privacy must be shared with IT to reflect in their compliance systems.
- **Incident Handling:** If an employee is under investigation or disciplinary review, HR must inform IT to monitor systems or restrict access if necessary.

📌 Final Note

These guidelines are reviewed quarterly and reflect the values of accountability, security, empathy, and innovation. All employees are expected to adhere to these rules diligently. Non-compliance may result in disciplinary action, including but not limited to termination of employment.

The InfoFlow AI leadership appreciates your role in maintaining a productive, secure, and respectful workplace.