IT Policy Manual

1. Purpose

This IT Policy Manual provides guidelines for the acceptable use of IT systems, software, hardware, and data across the organization.

2. Scope

Applies to all employees, contractors, and third-party users accessing organizational IT resources.

3. Acceptable Use Policy

- Use IT assets only for authorized work-related activities.
- Personal usage should be minimal and not interfere with productivity.
- Prohibited: accessing offensive content, pirated software, or unauthorized cloud services.

4. Software & Licensing

- Only approved software may be installed.
- Employees must not duplicate or share licensed software.

5. Email & Communication

- Business email accounts must be used professionally.
- No phishing, spam, or chain emails.
- Confidential information must not be sent unencrypted.

6. Data Backup & Retention

- Regular automated backups are taken.
- Users are responsible for saving data to approved drives.

7. Password Policy

- Minimum 8 characters, must include alphanumeric and special characters.

- Change passwords every 90 days.

- Never share passwords.

8. Reporting IT Issues

- All issues must be reported to IT Helpdesk within 24 hours.

HR FAQs

1. What are the working hours?

Standard working hours are 9:00 AM - 6:00 PM, Monday to Friday.

2. How do I apply for leave?

Leave requests must be submitted through the Employee Self-Service Portal and approved by your reporting manager.

3. What is the dress code?

Smart casuals from Monday to Thursday. Friday is casual day.

4. How is performance reviewed?

Annual performance appraisals occur in March, with mid-year reviews in September.

5. Who should I contact for HR-related queries?

Email hr@company.com or visit the HR desk on the 2nd floor.

6. What is the probation period?

Typically 6 months, after which performance is reviewed for confirmation.

7. Are there learning and development programs?

Yes. Employees can enroll in internal workshops, certifications, and online training platforms.

Security Policy

1. Purpose

This policy outlines the information security controls to safeguard company data and infrastructure.

2. User Access Control

- Access granted on least privilege basis.

- All users must have unique login credentials.

- Inactive accounts are deactivated after 30 days.

3. Network Security

- Firewalls, VPNs, and endpoint protections are enforced.

- Unauthorized USB or external devices are not allowed.

4. Data Protection

- All confidential data must be encrypted at rest and in transit.

- Sensitive files should be stored only on approved servers.

5. Incident Response

- Employees must report breaches, phishing attempts, or suspicious activity immediately to security@company.com.

- An incident response team will investigate and mitigate risks.

6. Mobile Device Policy

- Devices must be password-protected and can only connect through secure Wi-Fi.

- Remote wipe capability must be enabled.

7. Physical Security

- Access to server rooms is restricted.

- ID badges must be worn at all times.