IT Policy Manual

IT POLICY MANUAL

1. PURPOSE

This manual provides guidance for the effective use, management, and security of IT resources.

2. ACCEPTABLE USE

Employees must use IT resources for business purposes only. Unauthorized access, offensive content, and illegal downloads are prohibited.

3. EMAIL AND COMMUNICATION

Emails should be used professionally. Company email must not be used for personal gain or to spread malware/spam.

4. PASSWORD MANAGEMENT

Passwords must be strong and updated every 90 days. Sharing passwords is strictly prohibited.

5. DATA BACKUP

All company data should be backed up regularly. IT will ensure daily and weekly backups are stored securely.

6. SOFTWARE INSTALLATION

Only authorized personnel may install or remove software. Use of pirated or unlicensed software is forbidden.

7. INTERNET USAGE

Internet access should be used responsibly. Accessing harmful or non-business related content is not allowed.

8. DEVICE MANAGEMENT

All devices must be approved and registered with IT. Lost or stolen devices must be reported immediately.

9. MONITORING

The company reserves the right to monitor IT systems to ensure compliance with this policy.

10. VIOLATIONS

Policy violations may result in disciplinary action, including termination or legal prosecution.