IT Assistant Documents

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.