IT Security Policy Outline

1. Purpose

- Describe the intent and scope of the IT Security Policy.

2. Scope

- Define which areas, systems, and personnel are covered by the policy.

3. Roles and Responsibilities

- List responsibilities of IT staff, management, and end users.

4. Acceptable Use Policy

- Outline acceptable and unacceptable uses of company IT resources.

5. Access Control

- Describe user authentication and authorization requirements.
- Define privilege levels and access rights.

6. Data Protection

- Specify data classification, handling, storage, and disposal guidelines.

7. Network Security

- Provide requirements for network access, monitoring, and protection.

8. Physical Security

- Detail security controls for physical access to IT systems and infrastructure.

9. Security Awareness and Training

- Outline employee training and awareness requirements.

10. Incident Response

- Describe the process for reporting and responding to security incidents or breaches.

11. Business Continuity and Disaster Recovery

- Explain strategies for backup, recovery, and continuity of IT services.

12. Policy Review and Maintenance

- State how and when the policy will be reviewed and updated.

Document Control

- Date Issued:

- Version:
- Approved by:
- Next Review Date: