Organizational IT Security Policy

1. Purpose

Describe the purpose and objectives of this IT Security Policy.

2. Scope

Define the scope of the policyâ€”what systems, information, and employees are covered.

3. Policy Statement

Summarize your organization's commitment and approach to IT security.

4. Roles and Responsibilities

Role	Responsibility
IT Department	Oversee implementation, maintenance, and monitoring of security controls.
Management	Approve and support security policies and allocate resources.
All Employees	Comply with policies, report incidents, and protect organization assets.

5. Acceptable Use Policy

- Acceptable use of devices, network, and data resources.
- Prohibited activities (e.g., illegal downloads, sharing credentials).

6. Access Control

- User account creation and removal procedures.
- Password standards and multi-factor authentication requirements.
- Principle of least privilege.

7. Data Protection

- Data classification guidelines.
- Encryption and backup procedures.
- Retention and disposal of sensitive information.

8. Physical Security

- Access controls for facilities and server rooms.
- Visitor log procedures.

9. Incident Response

1. Report suspected or actual security breaches promptly.
2. Incident logging, investigation, and resolution process.

10. Policy Review and Updates

- Frequency of policy review.
- Update and approval procedures.

11. Enforcement

- Consequences of policy violations.
- Reporting violations and disciplinary actions.

12. Acknowledgement

Employees must acknowledge that they have read and understood the policy.