Information Security Policy

Document Version: _____

Last Reviewed: __/__/____

Approved By: _____

1. Purpose

State the purpose of the policy and its role in protecting information assets.

2. Scope

Describe the scope of the policy (e.g., all employees, contractors, IT systems, data, etc.).

3. Policy Statement

Summarize the company's commitment to information security.

4. Roles and Responsibilities

Role	Responsibility
IT Manager	*Define and maintain security controls.*
All Employees	*Comply with security policies and report incidents.*

5. Acceptable Use

- *Define acceptable and unacceptable use of IT resources.*
- *Reference to device, email, Internet usage, etc.*

6. Access Control

- *Outline requirements for user authentication and authorization.*
- *Include password recommendations, least privilege, etc.*

7. Data Protection

1. *Specify requirements for data classification and handling.*
2. *Data backup and recovery guidelines.*

8. Physical Security

Guidelines for securing physical access to IT assets.

9. Incident Management

Procedures for reporting and handling security incidents.

10. Policy Compliance

- *Consequences of policy violation.*
- *Monitoring and audit activities.*

11. Policy Review and Maintenance

Frequency and responsibility for reviewing and updating this policy.

12. References

- *List related policies, standards, and relevant legal/regulatory requirements.*

13. Approval

*Name:*_____
*Title:*_____
*Signature:*_____
*Date:*__/__/____