

Data Security Policy

Policy Number: [Policy Number]

Effective Date: [Effective Date]

Review Date: [Review Date]

Approved By: [Approver Name/Title]

1. Purpose

[State the objective and purpose of the policy]

2. Scope

[Define the scope of applicability: departments, systems, data types, personnel, etc.]

3. Policy Statement

[Provide an overarching security statement and goals]

4. Roles and Responsibilities

Role	Responsibility
Data Owner	[Description of responsibilities]
IT Department	[Description of responsibilities]
End Users	[Description of responsibilities]

5. Data Classification

- Confidential
- Internal Use
- Public

[Provide criteria for each classification]

6. Data Handling

- Collection
- Processing
- Storage
- Access Control
- Transmission
- Destruction/Disposal

[Describe handling requirements for each stage]

7. Access Control

- User authentication and authorization
- Role-based access

- Least privilege principle

8. Physical Security

[Physical access control, secure disposal of hardware, etc.]

9. Incident Management

[Procedures for reporting, responding, and documenting security incidents]

10. Training and Awareness

[Regular training requirements for staff]

11. Policy Compliance

[Monitoring, enforcement, disciplinary actions]

12. Exceptions

[Process for granting and documenting exceptions to the policy]

13. Review & Revision History

Date	Version	Description
[Date]	[Version]	[Summary of changes]