Data Encryption Policy Sample

1. Purpose

The purpose of this policy is to establish requirements for encrypting data to protect the confidentiality and integrity of information handled by [Organization Name].

2. Scope

This policy applies to all employees, contractors, and third-party service providers who have access to organizational data, regardless of the device or location.

3. Encryption Requirements

- All sensitive data at rest must be encrypted using approved cryptographic algorithms.
- All sensitive data in transit across public networks must be encrypted.
- Encryption keys must be generated, stored, and managed securely.

4. Acceptable Encryption Standards

Data Type	Encryption Standard
Files at Rest	AES-256
Data in Transit	TLS 1.2 or higher

5. Key Management

1. Encryption keys must be kept separate from encrypted data.
2. Keys must be rotated annually or immediately upon suspected compromise.
3. Access to keys is restricted to authorized personnel only.

6. Roles and Responsibilities

- IT Department: Implements and maintains encryption mechanisms.
- Employees: Comply with data handling and encryption procedures.

7. Policy Review

This policy will be reviewed annually and updated as needed to ensure continued suitability and effectiveness.

8. Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract.

Approval

Approved by: _____

Date: _____