

IT Data Protection Policy Template

1. Purpose

This policy provides the framework for protecting data managed by [Organization Name], ensuring compliance with applicable laws and regulations, and supporting best practices in data handling and security.

2. Scope

This policy applies to all employees, contractors, consultants, and partners who have access to [Organization Name]'s information systems and data assets.

3. Policy Statement

[Organization Name] is committed to ensuring the confidentiality, integrity, and availability of its data and information systems by implementing appropriate data protection measures.

4. Roles & Responsibilities

Role	Responsibility
Data Owner	Ensures data classification, access rights, and compliance with policies.
IT Administrator	Implements technical controls and monitors data protection mechanisms.
All Users	Responsible for following data protection procedures and reporting incidents.

5. Data Classification

- Confidential: Sensitive business and personal data, strictly controlled.
- Internal Use: Information accessible by employees but not public.
- Public: Information intended for public disclosure.

6. Data Handling Procedures

- Only authorized personnel may access sensitive data.
- Data must be encrypted at rest and in transit where applicable.
- Data-transfers outside the organization require management approval.
- Physical documents must be stored securely.
- Dispose of data safely when no longer required.

7. Data Breach Management

- Report any suspected or actual data breach immediately to IT.
- IT will investigate and document the incident.
- Notifying affected individuals and regulatory bodies as needed.

8. Compliance & Review

- This policy will be reviewed annually or as required by regulatory changes.
- Non-compliance may result in disciplinary action.

9. Approval

Date: _____

Signature: _____

Name & Position: _____