Organization Data Security Policy Draft

1. Purpose

This Data Security Policy defines the requirements and responsibilities for ensuring the security, integrity, and confidentiality of data handled by *[Organization Name]*.

2. Scope

This policy applies to all employees, contractors, systems, and data owned or managed by *[Organization Name]*.

3. Roles & Responsibilities

- Data Protection Officer: *[Name/Title]*
- Department Managers: Ensure compliance within teams
- All Employees: Adhere to security guidelines

4. Data Classification

1. Sensitive Data: *[Define sensitive data types]*
2. Confidential Data: *[Define confidential data types]*
3. Public Data: *[Define public data types]*

5. Data Handling & Access

- Access is restricted based on job roles.
- All access must be logged and reviewed regularly.
- Data transfer must use secure, encrypted methods.

6. Incident Response

- Report security incidents to: *[Contact/Procedure]*
- Document incidents and follow escalation procedures.

7. Training & Awareness

- All staff must complete security awareness training annually.
- Regular reminders will be distributed by the IT department.

8. Policy Review

- This policy will be reviewed every *[X]* months or upon significant changes.

Approval

Approved by: *[Name/Title]*

Date: *[Date]*