Data Security Governance Policy

Effective Date: [Insert Date]

1. Purpose

This Data Security Governance Policy establishes the framework for managing and safeguarding data to ensure confidentiality, integrity, and availability of information within [Firm Name].

2. Scope

This policy applies to all employees, contractors, and third parties who access, use, or manage company data.

3. Data Classification

- Confidential: Highly sensitive data requiring strict access control (e.g. client data, financial info).
- Internal Use: Information intended for use within the company (e.g. internal memos).
- Public: Information approved for general public disclosure.

4. Roles & Responsibilities

- **Data Owner:** Accountable for data protection and classification.
- **Data Custodian:** Responsible for implementing security measures.
- **User:** Obliged to follow security practices.

5. Data Protection

- Access to data is based on the principle of least privilege.
- Data must be protected using encryption in transit and at rest where applicable.
- Regular security awareness training is required for all users.

6. Incident Response

All security incidents must be reported to the Data Protection Officer immediately. Incident response processes will be initiated as per the firm's incident management procedures.

7. Policy Review

This policy will be reviewed and updated annually or as required by regulatory changes.

[Firm Name] Management