IT Governance Security Policy

1. Policy Statement

This document defines the framework for IT governance and information security within the Firm. The objective is to protect all information assets and support compliance with legal, regulatory, and contractual obligations.

2. Scope

This policy applies to all employees, contractors, and third-party users who access, manage, or handle the Firm’s information systems, infrastructure, and data.

3. Roles and Responsibilities

- **Board of Directors/Management:** Oversee policy enforcement and review.
- **IT Department:** Implement technical controls and monitor compliance.
- **Employees & Users:** Adhere to this policy and report incidents.

4. Access Control

- Ensure user access is based on business needs (principle of least privilege).
- Regularly review and update user access rights.
- Restrict administrative permissions to authorized personnel only.

5. Data Protection

- Protect data from unauthorized access, disclosure, alteration, and destruction.
- Classify information according to sensitivity and criticality.
- Establish procedures for data backup and recovery.

6. Incident Management

- Report security incidents promptly to the IT department.
- Establish procedures for responding to and investigating incidents.

7. Compliance

- Comply with applicable laws, regulations, and contractual requirements.
- Conduct regular security audits and assessments.

8. Policy Review

This policy will be reviewed annually or after significant changes to IT infrastructure or business processes.

9. Acknowledgment

All staff must read, understand, and adhere to this policy.

_____

_____

Authorized Signatory

_____

_____

Date