Information Security Policy

Version: 1.0

Owner: Security Governance Team

Effective Date: [Insert Date]

Last Reviewed: [Insert Date]

Purpose:

To establish a framework for managing the confidentiality, integrity, and availability of [Company Name]'s information systems and data.

Scope:

Applies to all employees, contractors, vendors, and systems that store, transmit, or access company data.

Policy:

- Information must be protected through access controls, encryption, and auditing.
- All users must use strong passwords and enable MFA where available.
- Systems and applications must be updated regularly to prevent known vulnerabilities.
- Data must be classified and handled according to the Data Classification Policy.
- All personnel must complete annual security awareness training.
- Incidents must be reported within 24 hours to the Security Team.

Enforcement:

Violations may result in disciplinary action, up to and including termination and legal penalties.

Review Cycle:

This policy shall be reviewed and updated annually or upon major system changes.