Document 1: Information Security Policy

1. Purpose

To establish guidelines for maintaining the confidentiality, integrity, and availability of organizational information assets.

2. Scope

Applies to all employees, contractors, and third-party users accessing organizational systems.

3. Policy Statement

Information must be protected against unauthorized access, disclosure, alteration, and destruction.

4. Roles and Responsibilities

- **Information Security Manager**: Develops, implements, and maintains security policies.
- **IT Department**: Enforces technical controls.
- **All Employees**: Adhere to security protocols and report incidents.

5. Access Control

5.1 User Authentication

- Strong password enforcement.
- Multi-factor authentication for sensitive systems.

5.2 Role-Based Access

- Access granted on a need-to-know basis.
- Periodic review of user privileges.

6. Data Classification

- Public
- Internal Use Only

- Confidential
- Restricted

7. Incident Response

- Report within 24 hours.
- Incident Response Team (IRT) investigates and mitigates.

8. Compliance

Regular audits and compliance with ISO/IEC 27001.