Security Compliance Policy

A security compliance policy defines rules and procedures to ensure compliance with security standards.

**Template Structure**:

1. **Title Page**
   * Document Title: "Security Compliance Policy"
   * Author: Rick Abraham
   * Date
2. **Policy Overview**
   * **Objective**: Purpose of the policy (e.g., to protect data integrity and ensure compliance with internal and regulatory requirements).
   * **Scope**: Specify areas covered (e.g., data storage, access controls, device security).
3. **Compliance Standards**
   * List the standards the organization must comply with (e.g., NIST, CIS, ISO 27001).
4. **Roles and Responsibilities**
   * Outline key roles involved in compliance (e.g., IT Administrator, Compliance Officer).
5. **Policy Statements**
   * Provide specific policy statements, such as:
     + **Access Control**: Only authorized personnel are allowed access to specific systems.
     + **Data Encryption**: All sensitive data must be encrypted during transmission and storage.
     + **Incident Reporting**: All security incidents must be reported to IT management within 24 hours.
6. **Compliance Monitoring**
   * Describe how compliance will be monitored (e.g., regular audits, automated monitoring tools).
7. **Enforcement and Penalties**
   * Outline potential consequences for non-compliance.