

# IT Security Compliance Policy Example

## 1. Purpose

This IT Security Compliance Policy outlines the measures and procedures required to safeguard the confidentiality, integrity, and availability of Company systems and data, and to ensure company-wide compliance with applicable legal, regulatory, and contractual security requirements.

## 2. Scope

This policy applies to all employees, contractors, and third-party users who access, process, store, or transmit company information and systems.

## 3. Policy

### 3.1 Access Control

- Users shall only have access required to perform their job responsibilities.
- Access rights must be reviewed at least quarterly.
- Default passwords must be changed upon initial login.

### 3.2 Data Protection

- All sensitive data must be encrypted both in transit and at rest.
- Backup copies of critical data must be maintained and tested regularly.

### 3.3 Network Security

- Firewalls and intrusion detection systems must be deployed and maintained.
- Unnecessary network services and ports must be disabled.

### 3.4 Incident Response

- All security incidents must be reported immediately to the IT Security Team.
- Incident response procedures must be documented and tested annually.

## 4. Compliance Requirements

1. Compliance with relevant laws and regulations (e.g., GDPR, HIPAA, PCI DSS).
2. Periodic security training for all employees.
3. Annual internal and external security audits.

## 5. Roles and Responsibilities

Role	Responsibility
IT Security Officer	Implementation and enforcement of security policies.
Managers	Ensure team compliance with security procedures.

## 6. Policy Review

This policy shall be reviewed and updated annually or as required to reflect changes to applicable laws, regulations, or business practices.

## 7. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Effective Date:** [YYYY-MM-DD]

**Approved By:** [Policy Owner Name/Title]