

# Security Policies and Governance Report

---

## Executive Summary

This report presents a structured security policy development framework covering Access Control, Data Protection, and System Use Policies. It also defines a governance structure with assigned roles and responsibilities for policy enforcement. Compliance is addressed by referencing the NIST Cybersecurity Framework (NIST CSF), and policy implementation is demonstrated with mock evidence showing how policies were communicated and enforced within a system.

---

## 1. Security Policy Development Framework

### Policy Document Name:

*Company X Information Security Policy*  
(Version 1.0, Effective Date: April 28, 2025)

---

### ◆ Access Control Policy

#### Purpose:

To restrict access to authorized users based on least privilege principles.

#### Policy Statements:

- All users must authenticate using company-approved methods (e.g., multi-factor authentication).
- Role-based access control (RBAC) must be applied to all internal systems.
- Default accounts must be disabled or renamed before production deployment.

#### Mock Implementation Logs:

text  
CopyEdit

```
April 28 09:10:33 server01 sshd[2398]: Accepted publickey for john.doe
from 10.1.1.100 port 56222 ssh2
April 28 09:11:04 server01 sudo:    john.doe : TTY=pts/0 ;
PWD=/home/john.doe ; USER=root ; COMMAND=/bin/ls
```

---

## ◆ Data Protection Policy

### **Purpose:**

To ensure the confidentiality, integrity, and availability of organizational data.

### **Policy Statements:**

- Sensitive data (e.g., PII, financial records) must be encrypted in transit and at rest using AES-256 encryption.
- External storage devices (USBs, external drives) are prohibited unless encrypted and approved by IT Security.
- Data retention policies must be enforced according to legal and business requirements.

### **Mock Evidence (Disk Encryption Status):**

```
bash
CopyEdit
sudo cryptsetup status data_partition
/dev/mapper/data_partition is active and is in use.
type: LUKS2
```

---

## ◆ System Use Policy

### **Purpose:**

To define acceptable use of organizational IT resources.

### **Policy Statements:**

- Users must not install unauthorized software or modify system configurations.
- Internet usage must align with professional responsibilities; non-business activities are prohibited during work hours.
- All activities on company systems are monitored and logged.

### **Mock Login Banner (Displayed on SSH Login):**

text

## 2. Governance Structure

**Security Governance Model:**

Hierarchical role assignment to ensure policy enforcement and oversight.

| Role                                      | Responsibilities  |
|---|---|
| CISO (Chief Information Security Officer) | Overall responsibility for information security governance, policy approval, and audits.            |
| IT Security Manager                       | Operational enforcement of policies, management of access controls, incident response coordination. |
| Department Managers                       | Ensure employee compliance within their departments; report policy violations.                      |
| All Employees                             | Adhere to security policies; complete mandatory security awareness training annually.               |

 Governance ensures accountability at every level.

---


## 3. Compliance Requirements

**Referenced Standard:**

- **NIST Cybersecurity Framework (NIST CSF)**

**Mapped to NIST CSF Functions:**

- **Identify:** Access Control policy supports asset management and governance.
- **Protect:** Data Protection policy aligns with data security and information protection processes.
- **Detect:** System Use policy supports security continuous monitoring.

 Aligning internal policies with NIST CSF ensures best practices and prepares for future audits.

---

## 4. Policy Implementation Evidence

### ◆ Communication

- **Training Conducted:**

- Mandatory "Acceptable Use and Data Protection" webinar held on **April 25, 2025**.
- 92% of employees completed training within the first week.

#### Mock Training Attendance Log:

| Employee Name | Completion Date |
|---------------|-----------------|
| John Doe      | 2025-04-26      |
| Jane Smith    | 2025-04-26      |
| Alex Brown    | 2025-04-27      |

---

### ◆ Enforcement

- **System Changes Made:**

- Implemented SSH login banner for legal notification.
- Enabled disk encryption using **LUKS** on critical servers.
- Configured audit logging on all production servers (**/var/log/audit.log**).

#### Mock Audit Log (Sample Entry):

```
log
CopyEdit
type=USER_LOGIN msg=audit(1651135200.123:231): pid=1234 uid=1000
auid=1000 ses=2 msg='op=login id=1000 exe="/usr/sbin/sshd"
hostname=10.1.1.100 addr=10.1.1.100 terminal=ssh res=success'
```

---

## Appendix

## Tools Used:

- `cryptsetup` (for data encryption)
  - `iptables` (for network access control)
  - `auditd` (for system use monitoring)
- 

## Final Notes

Through a structured framework based on industry standards, this project establishes robust security policies covering access, data protection, and system use. Governance responsibilities are clearly defined to ensure enforcement, and real-world examples (mock data) demonstrate effective policy rollout and monitoring.