Developing and Implementing Security Policies and Governance

In this project, I led the development and implementation of a comprehensive security governance framework for a small organization with approximately 75 employees. My goal was to build a sustainable and enforceable system that ensures confidentiality, integrity, and availability of information assets. The project was broken down into four major deliverables: creation of a formal security policy, governance structure, compliance alignment, and enforcement mechanisms.

1. Security Policy Document (Expanded)

I developed an official **Information Security Policy (ISP)**, documented in a 26-page handbook, that covers core security principles and practices. It was designed to be both accessible and enforceable.

📘 **Full Handbook Table of Contents:**

1. Introduction and Purpose
2. Scope
3. Definitions
4. Access Control Policy
5. Data Protection Policy
6. System Use Policy
7. Security Training and Awareness
8. Incident Response
9. Business Continuity and Disaster Recovery
10. Policy Review and Maintenance
11. Acknowledgment Form

🛡️ **Access Control Policy (Details)**

- **Authentication:** All users must use MFA (Microsoft Authenticator or YubiKey).
- **Account Creation:** Requests for new accounts require written approval from Department Head and IT.
- **Principle of Least Privilege:** Permissions granted only as necessary; group-based roles are audited monthly.
- **Logging:** Audit logs stored in Azure Sentinel for 180 days minimum.
- **Sample Log Extract (Azure AD):**

User: j.doe@org.com
Action: Elevated privileges
Time: 2025-02-14T10:23:11Z
IP Address: 10.1.2.45
Outcome: Success
Reviewer: IT Manager - Approved

🔐 **Data Protection Policy (Details)**

- **Encryption Standards:**
  - At Rest: AES-256 (BitLocker on endpoints, Azure Storage encryption)
  - In Transit: TLS 1.3 enforced via GPO
- **Backup Schedule:**
  - Nightly full backup at 1 AM
  - Stored in Azure Vault (Geo-redundant storage)
- **Data Classification Levels:** Confidential, Internal Use, Public
- **Policy Playbook for Data Breach:**
  - Identify affected assets
  - Isolate endpoint
  - Notify CISO and external auditors (if applicable)
  - Begin recovery procedures

💻 **System Use Policy (Details)**

- **Acceptable Use Policy (AUP):** Signed digitally by all users (DocuSign integrated with onboarding)
- **Device Monitoring:** Microsoft Defender for Endpoint logs:

Host: LAPTOP-JDOE
Activity: USB device connected
Time: 2025-03-03T13:12:02Z
Device: SanDisk Cruzer 32GB (Blocked by policy)

- **Prohibited Activities:** Personal file sharing, social media (unless approved), unauthorized software installations

2. Governance Structure (Detailed)

Security governance requires clearly defined roles and accountability. I created a governance chart and wrote Standard Operating Procedures (SOPs) for each role.

📊 **Governance Hierarchy:**

- **Chief Information Security Officer (CISO):**
  - Develops and maintains the ISP
  - Approves exceptions to policies
  - Coordinates incident response
- **IT Manager:**
  - Implements technical controls
  - Performs monthly access reviews
  - Maintains system logs and reports
- **Compliance Officer:**
  - Conducts internal audits every 6 months
  - Liaises with external compliance bodies
- **Department Heads:**
  - Ensure team adherence to the ISP
  - Report suspicious activity

- **End Users:**
  - Complete onboarding + annual training
  - Report incidents to IT within 24 hours

📄 **Sample SOP Excerpt - IT Manager Weekly Checklist:**

☑ Review admin privilege logs
☑ Validate backups completed and verified
☑ Patch compliance check on all devices
☑ MFA configuration audit in Azure

3. Compliance Requirements (Detailed)

We adopted the **NIST Cybersecurity Framework (CSF)** as our benchmark. I mapped our controls directly to NIST categories.

🔍 **Mapping Table:**

NIST CSF Category	Implementation Detail
PR.AC-1	Role-based access controls via Azure AD
PR.DS-1	Data encrypted at rest and in transit
DE.CM-1	Real-time monitoring via Defender, Intune
RS.RP-1	Incident Response Plan authored and distributed
RC.IM-1	Annual BCP testing and backup restores

📘 **Reference:**

- National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.
- Used crosswalk document to align internal policy with NIST CSF core functions.

4. Policy Implementation (Detailed)

📣 **Communication Strategy:**

- Policy uploaded to SharePoint and emailed via internal distribution list.
- Held a 1-hour virtual training (recorded, with transcript)
- Conducted a 10-question quiz via Google Forms (average score: 92%)
- Created quick-reference one-pagers for each department

🛠️ **Enforcement Strategy:**

- **Access Control:**
  - Configured Conditional Access policies:
    - Require MFA for all sign-ins from non-corporate IPs
    - Block legacy authentication protocols

- **Data Protection:**
  - Azure Information Protection labels applied to all documents
  - Admins auto-enforced encryption for USB storage using Intune policies
- **System Use:**
  - Microsoft Intune compliance profiles:
    - Require BitLocker
    - Require antivirus + firewall enabled
  - Deployed endpoint alert rules:

Alert: Unauthorized Software Installation
Device: DESKTOP-JSMITH
App: uTorrent.exe (Quarantined)
Response: User warned, supervisor notified

📸 **Collected Evidence (Documentation):**

- Screenshots of Azure policies and Conditional Access rules
- PDF export of all training attendance and quiz scores
- Intune device compliance report (CSV)
- Sample signed AUP forms (redacted)