SECURITY POLICY DEVELOPMENT

Project Overview

Understanding Security Policies and Their Foundations

Security policies are foundational documents that guide an organization's approach to **data protection**, **access control**, **incident response** and overall cybersecurity governance.
Before drafting any security policy, it's important to understand the key elements that influence how policies are created and enforced.

- **Laws** – Legal requirements an organization must follow when handling sensitive data.
- **Standards** – Industry frameworks like NIST and ISO that provide structured controls.
- **Policies** – High-level rules and expectations for employees, systems, and data.
- **Procedures** – Detailed step-by-step instructions that operationalize a policy.

This project explores each of these components and demonstrates how to use frameworks and templates to create professional grade policies for an organization named **Bayotech Solutions.**

1. Laws (Legal Requirements)

In cybersecurity, **laws** define the legal responsibilities organizations must follow when handling data, especially **Personal Identifiable Information (PII)**.

For individuals, data loss (e.g., losing a credit card or forgetting a password) typically affects only the person involved.
But when **organizations** collect, process, or store PII, they become **legally accountable** for protecting it.

Different regions and industries enforce different regulations, such as:

- **GDPR** –General Data Protection Regulation (EU)

- **HIPAA** –Health Insurance Portability and Accountability Act (Healthcare)
- **FedRAMP** –Federal Risk and Authorization Management Program (US Government)
- **PCI DSS** –Payment Card Industry Data Security Standard (Financial/Payment data)

These laws dictate **what organizations must do** to protect sensitive data.

2. Standards (Industry Frameworks)

Standards are industry bodies that help interpret and simplify the complexity of laws. They provide structure, best practices, and clear controls organizations can follow.
Major security standards include:

- NIST (National Institute of Standards and Technology)
- ISO 27001 (International Organization for Standardization)
- COBIT (Control Objectives for Information and Related Technologies)

Instead of every company trying to interpret laws independently (which would lead to inconsistency), these standards provide tested, approved templates and guidance.
They help organizations align with legal requirements and implement best practices.

3. Policies (High-Level Organizational Rules)

Security policies are official organizational rules created to enforce standards and comply with laws.
Policies can be internal or external:

- External Example: Facebook's Privacy Policy explains how the company collects and uses data.
- Internal Example: Company Acceptable Use Policy (AUP), data classification policy, AI usage policy, etc.

Policies tell employees and users what is allowed, what is prohibited, and what expectations must be met.

4. Procedures (Step-by-Step Instructions)

Procedures are detailed, actionable steps that explain how to implement a policy.
Examples:

- How to onboard a new employee
- How to assign a company PC
- How to add a user to a domain
- How to respond to an incident
- How to provision a cloud asset

Policies state what must be done;
Procedures explain how to do it.

Why Policies Matter

Security policies are often built using templates provided by industry-standard bodies like ISO, NIST, and COBIT.
These templates help ensure that an organization complies with relevant laws and regulates how data is handled.
Ultimately, everything in cybersecurity ties back to compliance.
If an organization collects or manages people's data, it must follow these rules and demonstrate compliance through:

- vulnerability scans
- risk assessments
- logging and monitoring
- incident response
- proper data handling
- secure system configuration

Tools & Security Policy Templates

ISO 27001 Templates→ ISO provides professional-grade policy and documentation toolkits.
These usually require a paid subscription but are widely used across industries.

You can search:
“ISO 27001:2022 Policy Templates Toolkit”

SANS Institute Templates → SANS provides **free** high-quality policy templates.

Steps to access them:

1. Visit the **SANS website**
2. Go to **Community Resources**
3. Select **Policy Templates**
4. Search for a policy type (e.g., “Acceptable Use Policy”)
5. Review available templates (Governance, Applications, Networks)
6. Download the **.docx** file

You can see publication dates and descriptions to ensure you’re using updated guidance.

Conclusion

This project showcases key Governance, Risk, and Compliance skills. And demonstrates my ability to:

- Write and interpret policies
- Understand compliance frameworks
- Align security practices with legal and industry requirements
- Build documentation used in real enterprise environments.