Name: JAY ARRE TALOSIG
Subject & Section: CTINASSL – COM231
Professor: Mr. Gaudencio Jeffrey G. Romano

Activity #3: LEC-AC3: Information Security Policy and Information Security Standard

1. Discuss the critical distinction between an Information Security Policy and an Information Security Standard.

A. **Information Security Policy -** Ito yung high-level document na galing sa Senior Management. Basically, sinasabi nito kung ano ang gusto nilang mangyari at bakit importante yun, pero wala itong technical details.

  - ***Example:*** Sasabihin lang sa Policy na "All employees must secure their workstations." General statement lang siya na nagse-set ng direction at authority.

B. **Information Security Standard -** Ito naman yung specific rules na mandatory sundin para ma-meet yung policy. Ito yung nagde-define ng how to do it. Mas technical ito at detalyado.

  - ***Example:*** Para supportahan yung policy sa taas, sasabihin sa Standard na: "Workstations must have an automatic screen lock set to 5 minutes of inactivity."

In short: Ang Policy ay ang "Strategy" (Direction), habang ang Standard ay ang "Tactics" (Rules).

2. Explain the hierarchical relationship between the two and how they collectively form the governance framework for an organization's security posture.

Imagine mo siya as a pyramid structure: nasa tuktok ang **Policy** at directly below it ay ang **Standards.**

- **The Hierarchy:** Yung Policy ang nagsisilbing "Constitution" or foundation. Siya ang nagbibigay ng authority. Kapag walang policy, walang legal basis ang IT team para mag-enforce ng rules. Yung Standards naman ang nagta-translate nung general intent ng management into specific, measurable technical requirements.
- **How They Form the Governance Framework:** Together, bumubuo sila ng complete loop para maging effective ang security posture ng organization**:**

  1. **Direction:** Si Policy ang nagsasabi kung ano ang risk appetite ng company (Governance).

2. **Execution:** Si Standard ang nag-eensure na consistent ang pag-apply ng security controls sa lahat ng systems (Compliance).

Kumbaga, yung Policy ang nagsasabing "Drive Safely" (Goal), at yung Standard ang nagsasabing "Do not exceed 60 kph" (Rule). Kailangan mo pareho para maayos ang governance.