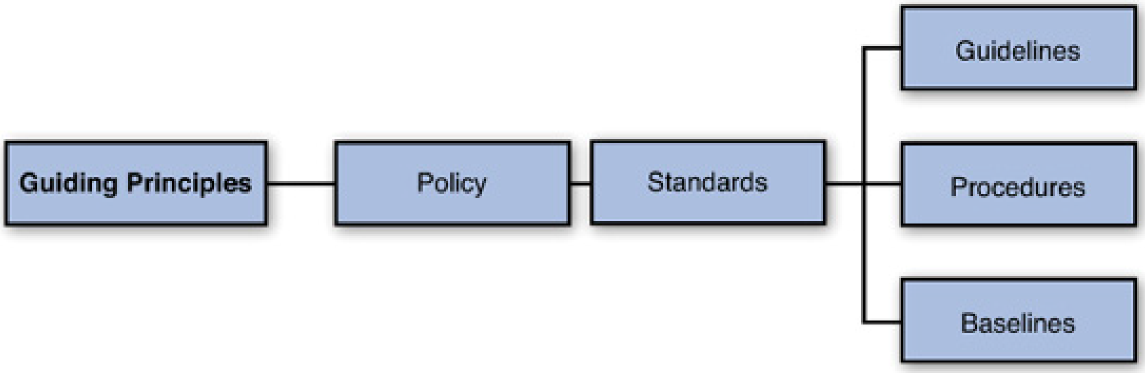
Ch.2 summary By @MHazazi

Policy Hierarchy

- Policies reflect the guiding principles and organizational objectives.

- ***A well-written policy*** clearly defines guiding principles, provides guidance to those who must make present and future decisions, and serves as an implementation roadmap.

Policy Hierarchy:
It is the relationship between a policy and its supporting documents.



What are these supporting documents ?
Standards, baselines, guidelines, and procedures support policy implementation.

Standards

Document that specify the implementation of policy and state mandatory requirements.

For example:
- every employee should have unique ID and password
- employee is not allowed to share his ID with anyone

- The standard is very specific to the infrastructure.
- Standards are determined by management,
- Standards are *not* subject to Board of Directors authorization.
- Standards change more often than policy

Baselines

An aggregate of implementation in standards and security controls for a specific category or grouping.

For example:
- All of our company computer platform is Windows OS.
- All of our management business mobile device should be company owned iPhone

- The primary objective of a baseline is uniformity and consistency.

Guidelines

Suggestion for the best way to accomplish a given task.

For example:
The following are general advices for creating a Strong Password:

- A Strong Password should be at least 10 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)

- Guidelines are created to assist users in implementing the policy
- Guidelines are *not mandatory*.

Procedures

Detailed document that explain the usage of guidelines and standers in step by step manner to meet the policy requirement.

For example:
To add a member to a local group using the Windows interface:

- Open Computer Management.
- In the console tree, click Groups .
- Right-click the group to which you want to add a member, click Add to Group , and then click Add

- Procedures focus on **actions or steps**.
- Procedures has four formats:
  - **Simple Step** = Lists sequential actions. There is no decision making.
  - **Hierarchical** = Generalized instructions for experienced users and detailed instructions for novices.
  - **Graphic** = Uses either pictures or symbols to illustrate the step.
  - **Flowchart** = Used when a decision-making process associated is with the task.

Plans and Programs

- Provides strategic & tactical instructions on how to execute an initiative or respond to a situation
- Plans are sometimes referred to as programs.
- Plans are closely related to policies.

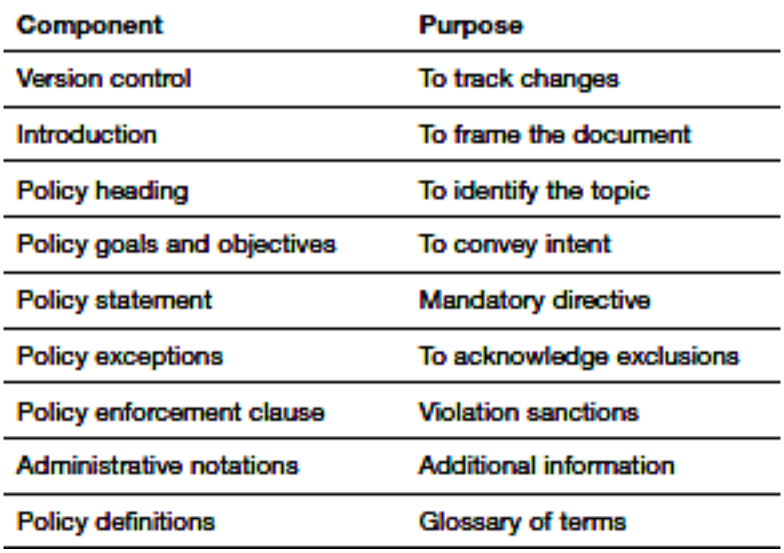
Examples : Vendor Management Plan, Incident Response Plan, Business Continuity Plan, Disaster Recovery Plan

Policy Formats

- **The style and format of policy will change based on targeted audience.**
  - Identify and understand the audience
  - Understand culture shared by audience
- **Plan the organization of document before you start writing**
  - One document with multiple sections? = consolidated policy ex. Governance Policy
  - Several individual documents? = singular policy ex. Information Security Officer Policy

Regardless of which format you choose, *do not* include standards, baselines, guidelines, or procedures in your policy document. If you include them you might have these problems:
Management challenge , Difficulty of updating , Cumbersome approval process

Policy Components



Component	Purpose
Version control	To track changes
Introduction	To frame the document
Policy heading	To identify the topic
Policy goals and objectives	To convey intent
Policy statement	Mandatory directive
Policy exceptions	To acknowledge exclusions
Policy enforcement clause	Violation sanctions
Administrative notations	Additional information
Policy definitions	Glossary of terms

Version control	- identified by a number or letter code - Major revisions 1.0 , 2.0 , 3.0 - Minor revision 1.1 , 1.2 , 1.3 - Version control documentation includes: • Change date • Name of the person(s) making the change • Brief synopsis of the change • Who authorized the change • The effective date of the change
Introduction	- Provides context and meaning - Explains the significance of the policy - Explains the exemption process and the consequences of noncompliance - Reinforces the authority of the policy - A separate document for a singular policy - Follows the version control table and serves as a preface for consolidated policy
Policy Headings	- identifies the policy by name and provides an overview of the policy topic - the format and contents of heading significantly depend on the policy format **- Singular policy includes:** • Name of the organization or the division • Category, section, and subsection • Name of the author and effective date of the policy • Version number and approval authority **- Consolidated policy document** • Heading serves as a section introduction and includes an overview

Policy Goals and objectives	- What is the goal of the policy? - Introduces employee to the policy content and conveys the intent of the policy - One policy may have several objectives - Singular policy objective located in policy heading or body of the document - Consolidated policy objectives are grouped after the policy heading
Policy Statement	- Why does the policy exist? - What rules need to be followed? - How will the policy be implemented? **- High- level directive or strategic roadmap** • Focuses on the specifics of how the policy will be implemented • It's a list of all the rules that need to be followed • Constitutes the bulk of the policy • Standards, procedures, and guidelines are not a part of the Policy Statement. They can be referenced in that section
Policy exceptions	- Not all rules are applicable 100% of the time - Exceptions do not invalidate the rules, as much as they complement them by listing alternative situations - Language used in this section must be clear, accurate, and concise so as not to create loopholes - Keep the number of exceptions low
Policy Enforcement Clause	- Rules and penalty for not following them should be listed in the same document. - The level of the severity of the penalty should match the level of severity and nature of the infraction. - Penalties should not be enforced against employees who were not trained on the policy rules they are expected to follow.
Administrative Notations	- Provides a reference to an internal resource or refers to additional information - Include regulatory cross-references, the name of corresponding document (standard, guideline, and so on), supporting documentation (annual reports, job descriptions), policy author name and contact information.
Policy Definition	- The glossary of the policy document - Created to further enhance employee understanding of policy and rules - Renders the policy a more efficient document - The target audience(s) should be defined prior to the creation of the glossary - Useful to show due diligence of the company in terms of explaining the rules to the employees during potential litigation

WRITING STYLE AND TECHNIQUE

- **Sets the first impression (know the audience)**
- **Policies should be written using plain language:**
  - Simplest, most straightforward way to express an idea
  - Follow The Plan Language Action and Information Network (PLAIN) guidelines

Plain Language Techniques for Policy Writing(10 points):

1.Write for your audience.

2.Write short sentences. Express only one idea in each sentence

3.Limit a paragraph to one subject.

4.Be concise. Leave out unnecessary words.

5.Don't use jargon or technical terms when everyday words have the same meaning.

6.Use active voice.

7.Use "must" not "shall" to indicate requirements.

8.Use words and terms consistently throughout your documents.

9.Omit redundant pairs or modifiers.

10.Avoid double negatives and exceptions to exceptions. Many ordinary words have a negative meaning, such as "unless".