Ch.1 summary By @MHazazi

Policy

definite course of action or procedure selected to guide and determine present and future decisions.

* Policy Today

Organizations types:
profit, nonprofit and not-for-profit businesses, government agencies, institutions.

* Corporate culture

- is shared attitudes, values, goals, and practices that characterize a company, corporation, or institution.

Three classifications:

Negative: Workers do not feel comfortable and may not be safe; customers are not valued and may even be cheated.

Neutral: business neither supports nor hinders its employees; customers generally get what they pay for.

Positive: businesses that strive to create and sustain a welcoming workplace, truly value the customer relationship, partner with their suppliers, and are responsible members of their community.

In positive organizations, policy is viewed as an investment and a competitive differentiator for attracting quality employees and customers.

* Guiding principles

reflect corporate culture. make the fundamental beliefs of an organization and reflect the kind of company that an organization seeks to be.

INFORMATION SECURITY POLICY

what is the rule of policy in general?

codify guiding principles, shape behavior, provide guidance to those who are tasked with making present and future decisions, and serve as an implementation roadmap.

What is the rule of information security policy?

Document defines how the organization is going to protect its information assets and information systems, ensure compliance with legal and regulatory requirements.

What is the objective of information security policy?

protect the organization, its employees, its customers, and also vendors and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information, protect the integrity of the information, and ensure the availability of information systems.

Information: is data with context or meaning.
Asset is a Resource with a value

Information asset

Any information item, regardless of storage format, that represents value to the organization Customer data, employee records, IT information, reputation, and brand

* Policy Characteristics

Successful policies establish what must be done and why it must be done.

1- Endorsed—The policy has the support of management.

2- Relevant—The policy is applicable and support the organization goals.

3- Realistic—The policy make sense.

4- Attainable—The policy can be successfully implemented.

5- Adaptable—The policy can accommodate change.

6- Inclusive—The policy scope includes all relevant parties.

7- Enforceable— administrative, physical, or technical controls used to support, and enforced policy existence.

* The Role of Government

Government *intervention* is required in order to protect its critical infrastructure and its citizens. *Intervention* with the purpose of either restraining or causing a specific set of uniform actions is known as ***regulation***.

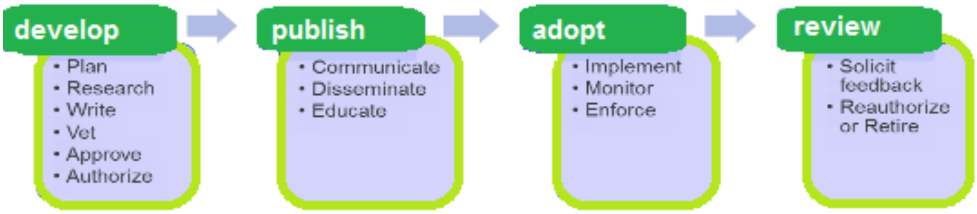
Two major information security-related legislations were introduced in the 1990s

1- Gramm-Leach-Bliley Act (GLBA) the Act was to reform and modernize the banking industry by eliminating existing barriers between banking and commerce.

2- The Health Insurance Portability and Accountability Act (HIPAA)

national standard to **protect individuals' electronic personal health information** (known as ePHI) that is created, received, used, or maintained by a covered entity, which includes healthcare providers and business associates.

INFORMATION SECURITY POLICY LIFECYCLE



Position	Board of Directors and/or Executive Management	Operation Management	Compliance officer	Auditor
Develop	Approve policy in addition to communicate and support the policy.	Policy planning, researching, writing, vetting, reviewing	Policy planning, researching, contributing, reviewing	Monitor policy compliance
Publish	Take the lead in demonstrating the policy via practice it, engorge it , and educate it to others.	Policy communication to others . Make it available to others. Raise the awareness about policy	Policy communication to others . Make it available to others. Raise the awareness about policy	Monitor policy compliance
Adopt	Policy and its implementation becoming a behavior for everyone.	Policy implementation, evaluation, monitoring, enforcement	Policy evaluation	Monitor policy compliance
Review	Reapprove policy or remove the old ones.	Feedback about policy, provide recommendation	Feedback about policy, Provide recommendation	Monitor policy compliance

Develop	➢ Identify the need to the policy (what is the reason behind this policy?) ➢ Outline legal, regulatory and operational requirements to aligned the policy with them. ➢ Identify your audience (write in proper language and style). ➢ Assess the policy with expert, IT SME, legal council and regulator. ➢ Review the policy with all impacted entities before authorizing the policy. ➢ Get the final authorization from the executive management or equivalent.
Publish	➢ Announce the policy through the management by telling everyone how impotent is this policy for the organization. ➢ Have the new policy available to people whom intended to. In case anyone would like to read and know more about it. ➢ Raise the awareness of the people about the released policy. Through (eLearning, training, presentation, feedback) to reinforce the importance of the policy.
Adopt	➢ ensure that everyone understands the policy and how to be implemented. ➢ Monitor the policy compliance and ensure form its implementation (audit, survey, interview, violation & incident report). ➢ Keep the momentum by reinforcing the policy regularly.
Review	➢ Review the policy every year, and take the feedback from internal and external, to have the policy keeping up with any changes in the organization or its infrastructure. ➢ Outdated policy should be updated to meet any changes within the organization or its infrastructure. If policy can’t be updated, then it should be removed.