CYBER SECURITY

UNIT 4

Information security policy

- **information security policy** is a documentation of organizational level decisions on safeguarding the information.

- A security policy **defines the rules** that regulate how your organization manages and protects its information and computing resources to achieve security objectives.
- Information security policy is used to protect the integrity, confidentiality and availability of organization.

- It’s the first, and one of the most critical, steps to securing your environment

.

Need for Information Security Policy

A security policy should fulfill many purposes. It should:

1. Protect people and information
2. Set the rules for expected behavior by users,system administrators, management, and security personnel
3. Authorize security personnel to monitor, probe,and investigate
4. Define and authorize the consequences of violation1
5. Define the company consensus baseline stance on security
6. Help minimize risk
7. Help track compliance with regulations and legislation

Challenges for security Policy

- Extremely difficult to develop, policy often unique to each organization.

- No common format or process for developing one.

- Making it simple so everyone can understand and use it.

- Getting management consensus.

- How do you enforce it?

Security Principles

- Ensure the availability of data and processing resources to everyone.

- Provide assurance for the confidentiality and integrity of customer data and allow for the compartmentalization of, substitution, insertion, and deletion of that data risk for customers and your organization.

- Ensure the integrity of data processing operations and protect them from unauthorized use.

- Ensure the confidentiality of the customer’s and your processed data, and prevent unauthorized disclosure or use.

- Ensure the integrity of the customer’s and your processed data, and prevent the unauthorized and undetected modification.

Purposes of a Security Policy

- The primary purpose of a security policy is to inform users, staff, and managers of those essential requirements for protecting various assets including people, hardware, and software resources, and data assets.

- The policy should specify the mechanisms through which these requirements can be met.

- Another purpose is to provide a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the policy.

Types of Security policies and their review process

- Review process is also essential to ensure that security policy is appropriate or adequate
- Various types of security policies and their review processes:-
  1. World wide web (WWW) Policy
  2. E-mail security policy
  3. Corporate Policy

WWW policy

1. No offensive or harassing material may be made available through company website
2. No personnel commercial advertising should be made available through company website
3. The personnel material on or accessible from the website should be minimal.
4. No company confidential material should made be available
5. Users of an organization should not be permitted to install or run web server

E-mail security policy

1. Not transmit unsolicited mass email (spam) not to anyone
2. Not send messages that are harassing, hateful or threatening
3. Not send any chain letter
4. Not send message that supports illegal or unethical activities
5. E-mail should not be used to send sensitive information
6. Not use email broadcasting facilities except for making appropriate announcements
7. Keep personal email use to minimum.
8. Keep Policy and procedures secured from abusers.
9. Will demonstrate the same respect to email communication as to verbal communication.
10. Will check grammar, spelling before send the message.

Corporate Policy

Corporate Policy is the formal declaration of the principles and polices according to which a company will operate .These policies and principles are prepared by board of directors of the company or senior management committee .

Corporate policy comprises:

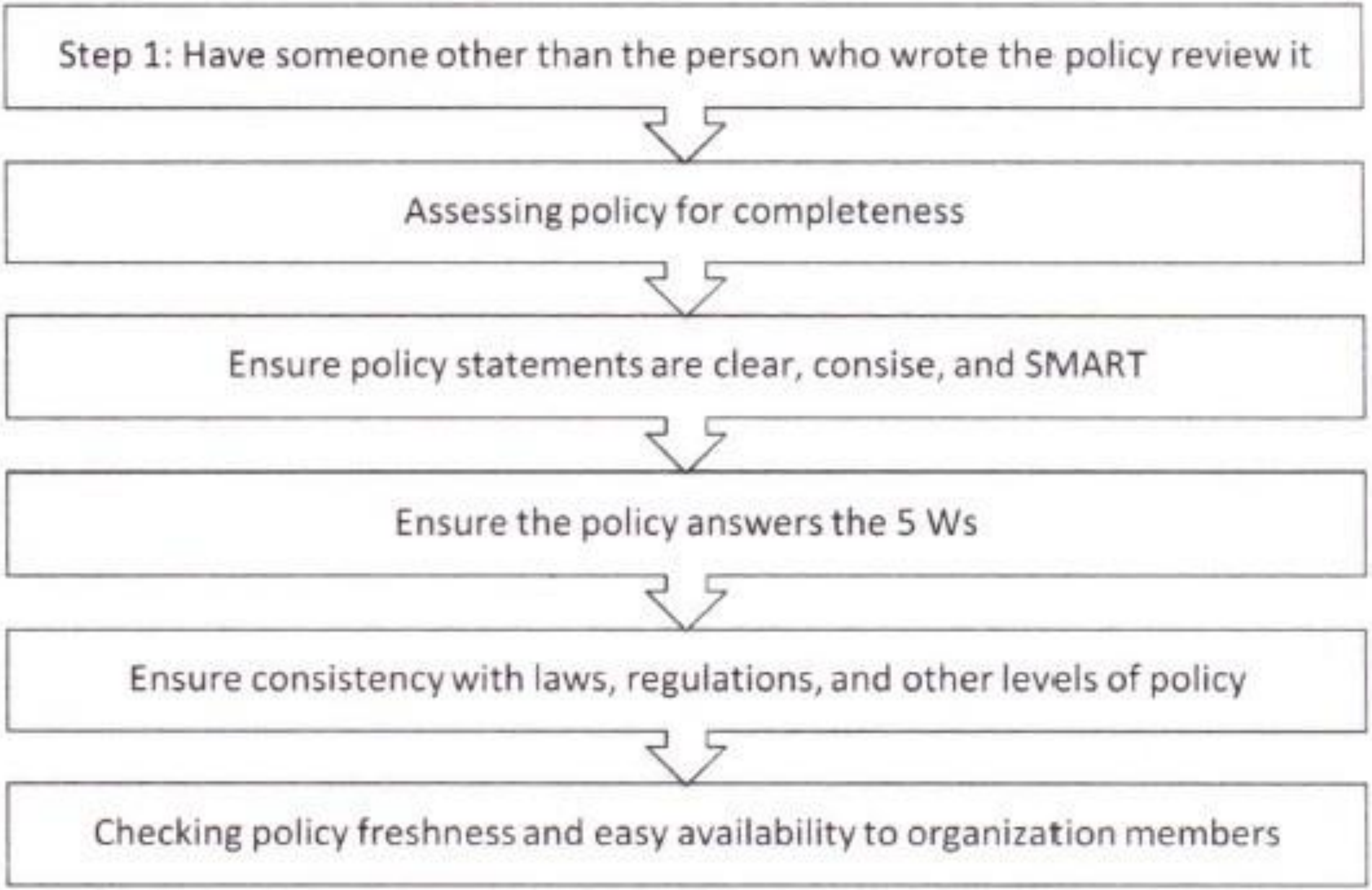
- Company’s mission statement
- Company’s objectives
- Principles on the basis of which strategic decisions are made

Policy Review Process

- Each policy created should be reviewed appropriately to ensure successful policy development.

- There are six important steps to be performed while evaluating information security policy:-

Policy Review Process



Step 1: Have someone other than the person who wrote the policy review it

Assessing policy for completeness

Ensure policy statements are clear, consise, and SMART

Ensure the policy answers the 5 Ws

Ensure consistency with laws, regulations, and other levels of policy

Checking policy freshness and easy availability to organization members