Security Policies

By Gerald Pine
What is a Security Policy?

- A security policy is a document that outlines the protections that should be enacted to ensure that the organization’s assets face minimal risks.

- Security policies, along with the accompanying procedures, standards, and guidelines, are keys to implementing information security in an organization. Having a written security policy empowers an organization to take appropriate action to safeguard its data.
A security policy does the following:

- Communicates a consensus of judgment.
- Defines appropriate behavior for users.
- Identifies what tools and procedures are needed.
- Provides directives for Human Resource action in response to inappropriate behavior.
- Helpful in the event that it is necessary to prosecute violators.
Security Policy Cycle

- The security policy cycle is a three phase process:
  - Vulnerability assessment cycle
  - Security policy cycle
  - Compliance monitoring and evaluation
Security Policy Life Cycle

- Vulnerability assessment is the first phase and contains the following steps:
  - Asset Identification-Determine which items need to be protected. Can include data, hardware, personnel, physical assets, and software.
  - Threat Identification-Determine the threat from threat agents (any person or thing with the power to carry out a threat against an asset).
Security Policy Life Cycle

- Vulnerability Appraisal-Determine what current security weaknesses that might expose the assets to the threats.
- Risk Assessment-Determine the damage that would result from an attack and the likelihood that the vulnerability is a risk to the organization.
Security Policy Life Cycle

- Risk mitigation: Once the risks are determined and ranked, the final step is to determine what to do about the risks. It is important to recognize that security weaknesses can never be entirely eliminated; some degree of risk must always be assumed.
Security Policy Life Cycle

- The second phase of the security policy cycle is to use the information from the risk management study to create the policy. The policy will clearly define the defense mechanisms an organization will employ to keep information secure.
Security Policy Life Cycle

- The final phase of the policy is to review for compliance. New assets and threats should always be taken into consideration. This process is ongoing and serves to identify new risks.
Security Policy Steps

- There are a set of principles to take when creating a security policy:
  - Be implementable and enforceable
  - Be concise and easy to understand
  - Balance protection with productivity
  - A good policy should be made by a group which includes an administrator, management, legal, and an end user.
Conclusion

- There are many steps to making a security policy and sometimes not everything is or can be included.
- Security policies are not only used to protect the organization but also to protect the employees as well.