What you need to know about Security Policy?

What is Security Policy?

Security policy is defined as a high-level statement of organizational beliefs, goals, and objectives and the general means for their attainment as related to the protection of organizational assets. It is brief, is set at a high level, and never states "how" to accomplish the objectives.

Why Implement Security Policy?

We live in a world where computers are globally linked and accessible, making digitized information especially vulnerable to theft, manipulation, and destruction. Security breaches are inevitable. Crucial decisions and defensive action must be prompt and precise. A security policy establishes what must be done to protect information stored on computers. A well written policy contains sufficient definition of "what" to do so that the "how" can be identified and measured or evaluated.

Without a security policy, any organization can be left exposed to the world. It is important to note that, in order to determine your policy needs, a risk assessment must first be conducted. This may require an organization to define levels of sensitivity with regard to information, processes, procedures, and systems.

What are the Components of a Security Policy?

When developing security policy, there is as much danger in saying too much as there is in saying too little. The more intricate and detailed the policy, the more frequent the update requirements and the more complicated the training process for those who adhere to it.

The components of a security policy will change by organization based on size, services offered, technology, and available revenue. However, most organizations have a guide which dictates the makeup of all company policies. This guide likely contains some or all of the following:

- Purpose – this section states the reason for the policy.
- Scope – this section states the range of coverage for the policy (to whom or what does the policy apply).
- Background – this section provides amplifying information on the need for the policy.
- Policy statement – this section identifies the actual guiding principles or what is to be done. The statements are designed to influence and determine decisions and actions within the scope of coverage.
- Enforcement - this section should clearly identify how the policy will be enforced and how security breaches and/or misconduct will be handled.

- Responsibility –this section states who is responsible for what. Subsections might identify who will develop additional detailed guidance and when the policy will be reviewed and updated.
- Related documents – this section lists any documents (or other policies) that affect the contents of this policy.
- Cancellation – this section identifies any existing policy that is cancelled when this policy becomes effective.

What determine a good Security Policy?

An organization may have a written policy, but it may be confusing and hard to read. It may also contain 'gaps' where some key issues are addressed, but others are not. In general, a good security policy does the following:

- Communicates clear and concise information and is realistic;
- Includes defined scope and applicability;
- Consistent with higher-level policy and guidance;
- Open to change based on new risks and vulnerabilities;
- Identifies the areas of responsibility for users, administrators, and management;
- Provides sufficient guidance for development of specific procedures
- Balances protection with productivity;
- Identifies how incidents will be handled; and
- Is enacted by a senior official.

A key point to consider is to develop a security policy that is flexible and adaptable as technology changes. Security policy should also be a living document routinely updated as new technology and procedures are established to support the mission of the organization. Additionally, organization should aware that the development of a security policy should be a collaborative effort with security officials, management, and those who have a thorough understanding of the business rules of the organization.

It is important to acknowledge that a security policy should not impede an organization from meeting its mission and goals. However, a good policy will provide the organization with the assurance and the acceptable level of asset protection from external and internal threats.