

SECURITY POLICY DEVELOPMENT

No Rules?

What if the meaning of Top Secret was: “Distribute this to anyone you trust, but not to those you don’t?” Would this protect a country’s valuable national defense secrets? Probably not! While most people understand the intent of such a statement, few could agree on whom to trust and not trust.

Yet, this is exactly what many organizations do when they develop an enterprise security program. Able technologists are given the directive to “make the company safe” without a clue as to what that really means. Moreover, a complex organization will have multiple points of entry, connectivity, and processing facilities, all managed by different groups. Yet, there is no consistent definition of what is considered “safe behavior”.

Missing the Forest for the Trees

The foundation of any enterprise security program is the policy. This singular statement answers the questions:

- Who?
- What?
- Where
- When?
- Why
- How?

Security Policy gives the “Why” to those who are responsible for developing the program. It ties together the efforts of multiple, disparate groups. And, this policy informs the rest of the organization of their responsibilities.

What Does a Policy Cover?

The policy itself may cover a global spectrum of subjects. These include:

- Data protection
- Customer privacy
- Network interconnection
- Software use
- Hardware configuration
- Facilities

The list will change for each organization. However, one important criterion for any policy is that it remains static and inclusive. It should not include details that are subject to frequent change, such as the model or version of a firewall or the cryptographic algorithm for a VPN. The policy should leave these details for more dynamic guidelines, subject to review and revision.

Guaranteeing Understanding

Just having a security policy is not enough. It is important to communicate it. It is here that Network & Security Technologies adds further value to your efforts. The best way to communicate is through the written word. It serves to provide statement to all that is not ambiguous. A policy document must explain:

- Affected Personnel
- Permitted activities
- Required activities
- Prohibited activities
- Consequences
- Reporting

Imposing such a structure makes the policy clear. Moreover, the writing should be direct and concise so that it is easy to understand.

Staying In Tune

One of the biggest policy mistakes many organizations make is to try to cover all the bases. As a result, few of those affected can use it. Instead, the policy should be relevant to the organization and the people who must implement it.

Finally, while the policy is not a dynamic document, it still needs to respond to the times. If it does not address the present threats it fails to protect. Thus, the policy must stay current.

Putting It All Together

Network & Security Technologies has experts who specialize in security policy development. These consultants know how to translate the requirements of business into policy statements. They have the experience and knowledge to ensure that our clients' organizations are not "handcuffed" by an overly paranoid security posture, yet protects itself from the real dangers that lurk on the e-Business playing field. They help to identify the appropriate level of risk that maximizes the rewards of using this most powerful modern medium. Most importantly, they translate these into a policy that is right for the client organization. Talented writers produce a final document that will not sit on the shelf. Rather, staff and management will make constant use of the most valuable tool in any enterprise's security program—the security policy.

A SECURITY POLICY IS...

- Static
- Understandable
- Supportable
- Clear
- Concise
- Relevant