

Guide to Developing a Security Policy

Developing a Security Policy is the first step you should take toward securing your network. A Security Policy lays the foundation for how you deal with security issues. Its purpose is to identify the resources that need to be protected, identify the people responsible for protecting them, and to identify who the policy covers. It should also state the consequences of policy violation and give general guidelines on how resources will be secured.

A Security Policy should be written so it doesn't require frequent modification. Details that require periodic change should be spelled out in more specific sub-policies (i.e. password policy, acceptable use policy, remote access policy). A good resource for examples and templates of specific policies can be found at <http://www.sans.org/resources/policies>. A Security Policy should be reviewed annually or when significant changes occur in technology or in your organization's strategic goals and business practices.

The development of a security policy requires input from all levels of an organization. Executive staff, management, technical staff, internal users and external customers will all have an interest. Obtaining input and support from all parties during the development of the security policy will make the process smoother and there will be less confusion and resistance during implementation. The involvement of all levels will also provide a more streamlined process for future decisions, when they become necessary.

There are several things you need to do before you develop your Security Policy. The first is to determine what resources need to be protected and what kinds of traffic will be allowed on your network. The next is to determine responsibilities and who the policy covers. You should identify the people authorized to make policy decisions and changes, and the people responsible for the technical implementation and ongoing management.

The final thing is to put the mechanisms in place that carry out or enforce the security policy. This step is when you decide which technical or non-technical solutions will best fit your needs. (Examples: If your policy states that you will block all incoming traffic, do you need a network firewall or will a personal firewall be sufficient? If your policy states that only approved software may be installed, do you take away all administrative rights on workstations or rely on users to voluntarily comply?) The security policy should be developed independently from any technical solution that will be used to enforce it. By keeping the security policy and technical solution separate, the policy will not be limited by the capabilities of the hardware or software of any specific device. The choice of the technology used should reflect the security policy not the other way around.

The success of your organization's security initiative is directly related to the existence of a well-thought-out and consistently-implemented security policy.

If you don't already have a security policy, the following questions should help you get started developing one. Since each organization will have different requirements, these questions are intended to cover the basics you should address.

Resource Questions

1. What resources or assets need to be protected?
 - Servers/workstations
 - Data

2. Are there any laws or regulations that you need to comply with or follow?
 - FERPA
 - HIPPA
 - CIPA

3. What services or shared applications are allowed to run on your network?
 - File Sharing
 - Printing
 - Database Services
 - Web site (internal access/external access)
 - Email server (internal access/external access)
 - FTP server (internal access/external access)
 - Video
 - Accounting Software
 - Student Record Software
 - Library Automation Software

4. What types of user traffic do you allow on your network?
 - Web browsing (work related/personal)
 - Email (work related/personal)
 - Peer-to-Peer file sharing
 - Instant Messaging
 - FTP
 - Telnet

5. Do you have Wireless on your network?

6. Do you allow remote access?
 - SSH
 - VPN
 - Terminal Services

PC Anywhere

Responsibility Questions

1. Who does the policy apply to?
 - a. Employees
 - b. Visitors
 - c. Vendors
2. Who is authorized to make policy changes?
3. Who is authorized to enforce the security policy violation consequences?

Implementation Questions

1. How will you secure workstations and servers from attacks from the Internet?
 - a. Network Firewall
 - b. Personal Firewall
 - c. Network Address Translation
2. How will you secure confidential information?
 - a. Limit access to database?
 - b. Require secure connection?
3. How will you authenticate users on your network?
4. How will you perform backups on your data?
 - a. Daily
 - b. Weekly

Additional Questions

1. What are the consequences for policy violation?
2. Do you allow personal devices on your network?
 - a. Personal laptops
 - b. PDAs
3. Do you run anti-virus software on all workstations and servers?
4. Are users allowed to install software on their workstation?
5. Do you require users to lock workstations when they are away from them?
6. Are servers and network equipment kept in a secure location?
7. Do you perform regular backups?
8. Where are your backups stored?
9. Are users required to attend security training?
10. Do users have an expectation of privacy?
11. Do you have a disaster recovery plan?
12. Do you have provisions in place to allow you to monitor the network at any time?

13. Do you have an incident response plan?
14. Do you have a copyright policy?
15. Do you have a change management policy?
16. Do you limit access to the buildings or rooms where servers are located?
17. How will exceptions to the security policy be handled?