

Guidelines for Developing a Security Policy

Security solutions work best when there is a company security policy in place that defines what is to be secured, how and by whom. As every company is unique, one policy will not work for all, but the process of creating a successful security policy can follow a set of guidelines.

- **Scope.** What information and systems need to be covered in this policy? Identify your critical information. What is its value to you? Only when you evaluate its value, can you determine the amount of resources you should employ to protect it.
- **Objectives.** What are the objectives? What do you hope to accomplish with this policy? What information do you want to secure? Who do you want to have access?
- **Security Parameters.** What security level should the company maintain? How much security do you need to have on the desktops, on the network servers and at the gateway to the internet? What access and security do people working remotely require?
- **Responsibility.** Who will be responsible for developing and maintaining the policy, informing all employees, technically implementing security and enforcing the policy? A team of managers might ultimately be responsible including the finance manager, human resource manager, and IT manager or computer/network consultant.
- **Rules, Rights, & Requirements.** Who has access rights to critical information? What are the requirements and rules to access confidential information? Which ones apply to employees and managers?
- **Information & Training.** What training needs to be done and how often?
- **Contingency Planning.** What happens when there has been a security breach? What happens when someone hasn't complied with the security policy? What routines should be in place to mitigate the damage?
- **Annual Review.** Does the policy need updating? What has changed? How well has the policy been observed?