



The Company Inspector - FAQ

Keeping Your Organization Secure

Frequently Asked Questions

General Questions.....	2
What is Information Security?	2
What is IT Security?	2
What should we do first to ensure IT Security?	2
How to identify your security requirements?	2
Security Policy	2
What is a Security Policy? How is it related to security standards, guidelines and procedures?.....	2
What should be considered first when drafting a security policy?	2
Who should be involved in development of a Security Policy?.....	3
How to develop a Security Policy?.....	3
What can I include into my Security Policy?	3
What are the benefits of having a Security Policy?.....	3
What should I consider when implementing Security Policy?.....	3
What is meant by Security Assessment?.....	4
What is a Security Audit?.....	4
How often should a Security Audit be performed?.....	4
Who should perform a Security Audit?	4

Computer Breakthrough, Inc.
101 Blanchard Road, Cambridge, MA 02138 (617) 354-7303



The Company Inspector - FAQ

Keeping Your Organization Secure

GENERAL QUESTIONS

What is Information Security?

Information Security refers to all aspects of protection for information. Most often, these aspects are classified in three categories: confidentiality, integrity, and availability of information. Confidentiality refers to the protection of the information from being disclosed to unauthorized parties while integrity refers to the protection of information from being changed by unauthorized parties. Availability refers to the information being available to authorized parties when requested.

What is IT Security?

There is no exact definition, but the general idea is to protect of any IT information and resources with respect to confidentiality, integrity and availability.

What should we do first to ensure IT Security?

It is recommended to use a systematic approach by first considering the security interest of the organization or department as a whole. You can first identify the security requirements of your organization, and then establish your security policy followed by enforcement. But periodic and continuous review and monitoring are definitely necessary in order to have an effective and efficient security policy.

How to identify your security requirements?

You can first identify what you are going to protect such as your equipment and assets. Then you can find out the threats, the impact of each threat and the chance of their occurrence. To identify the threats which are often of different natures, a process namely risk analysis is normally used. Through this process, you can identify what assets to protect, their relative importance, and the priority ranking for urgency and level of protection required. As a result, a list of security requirements can be defined for your organization.

SECURITY POLICY

What is a Security Policy? How is it related to security standards, guidelines and procedures?

Security policy sets the basic mandatory rules and principles on information security. It should be observed throughout an organization and should be in accordance with your security requirements and organization's business objectives and goals. Security standards, guidelines and procedures are tools to implement and enforce security policy such that more detailed managerial, operational and technical issues can be considered. Standards, guidelines and procedures may require more frequent reviews than security policy.

What should be considered first when drafting a security policy?

- Goals and direction of the organization.
- Existing policies, rules, regulations and laws of the Government.

Computer Breakthrough, Inc.

101 Blanchard Road, Cambridge, MA 02138 (617) 354-7303



The Company Inspector - FAQ

Keeping Your Organization Secure

- Organizations own requirements.
- Implementation, distribution and enforcement issues.

Who should be involved in development of a Security Policy?

Developing a Security Policy requires an active support and ongoing participation of individuals from multiple ranks and functional units. You can form a working group or task force to develop the Policy. But the exact group of personnel required depends on your organization's requirements. In general, this group may include empowered representatives from management, technical personnel, system developers, operational personnel, officers or users. Management represents the interests of the organization's goals and objectives, and can provide the overall guidance, assessment and decision making. Technical personnel can provide technical support for various security mechanisms or technological aspects. Users represent the users of related systems who may be directly affected by the Policy. Sometimes, a third party may get involved to review the Policy drafted.

How to develop a Security Policy?

You may first identify the group of people involved in developing the Policy. Second, make all necessary plans for activities, resources acquired and schedules. Then determine your security requirements, and establish your own Security Policy. You may need to go through several iterations of review and refinement for your Policy before a complete one can be established. As technology, environment and your requirements often change, you may need to continuously review and monitor your Security Policy in order to make it effective and useful for your organization.

What can I include into my Security Policy?

Typical contents may include the policy objectives and scope, the assets to be protected, the roles and responsibilities of the involved parties, the DO and DON'T rules and security incidents reporting and handling. However, the exact contents and level of details depend on your security requirements and your organization's business objectives. Before drafting your security policy you should also consider the existing policies, rules, regulations, laws, and your implementation, distribution and enforcement issues.

What are the benefits of having a Security Policy?

It gives us a yardstick to measure against. As mentioned before, you and your staff can clearly understand what is and is not permitted in your organization relating to the protection of IT resources. This also helps to raise the level of security consciousness and to provide a baseline on which detailed guidelines and procedures can be established. It may also help to support the decision of prosecution against security violations.

What should I consider when implementing Security Policy?

Of course, you must first observe your organization's procedures, rules and regulations for implementation. However, no policy is considered to be implemented unless users or related parties have commitment and communication. This can be done through briefing, orientation and ongoing training. Make them aware that the Policy can create benefits to their daily work and if possible, invite them to participate in the process of developing the Policy. This can gain their commitment and acceptance of the Policy.

Computer Breakthrough, Inc.
101 Blanchard Road, Cambridge, MA 02138 (617) 354-7303



The Company Inspector - FAQ

Keeping Your Organization Secure

What is meant by Security Assessment?

Security assessment here is defined as the methods to assess the security of the network or system. A security assessment software is specially designed to reduce the chance of internal abuse by searching and eliminating unnecessary security risks and vulnerabilities on internal hosts and workstations. These assessment tools are often used for security audit.

What is a Security Audit?

A security audit is performed in order to check and review the effectiveness and completeness of your security controls, your security policy, standards, guidelines and procedures. It will identify any inadequacies of the policy and related standards, and will find out if there are any security vulnerabilities of IT resources. Recommendations and remedy actions on security measures will be provided. In fact, a security audit should be an on-going process which should be performed periodically or regularly as there may be new vulnerabilities coming up daily.

How often should a Security Audit be performed?

A Security Audit only provides a snapshot of the vulnerabilities revealed at a particular point of time. But technology and your environment changes daily. There may be vulnerabilities found in the future even if all existing vulnerabilities have been identified. Periodic and ongoing review is inevitably required. Our standard audit is performed four times per year.

Who should perform a Security Audit?

A Security Audit is a complex task and requires skilled and experienced personnel. It must be planned carefully. Look for a company that has experience as well as the ability to translate the information into plain English.

Computer Breakthrough, Inc.
101 Blanchard Road, Cambridge, MA 02138 (617) 354-7303