

Security Policies & Procedures

Security Policies and Procedures are the backbone of information management and protection. Many organizations have no policies established, or their policies are so outdated they are ineffective. A current, practical Security Policy is essential to provide a framework for the deployment and management of your security infrastructure. We can help you design or update policies, standards and procedures to ensure an effective security framework is in place, incorporating security best practices.

Security Policies are effective only once they've been communicated to employees. Many companies fall short with their Policies by not implementing a thorough communication and awareness campaign. Security Policy Development and The Security Awareness Program are services provided by our Security and Disaster Recovery (DR) Team, one of the largest security teams in Atlantic Canada.

DESCRIPTION

We can provide your company with the knowledge and experience necessary to write a complete set of Security Policies that are tailored to the specific and unique needs of your company. These Policies will cover acceptable and unacceptable usage, administrative policies, server support and configuration policies, workstation policies, backup and recovery policies, networking, firewall and remote access policies, and much more. We design policies that allow for ease in maintenance, enabling an organization to keep their policies current and functional.

BENEFITS

Security Policies provide a framework for securing, deploying and managing the company's IT infrastructure. All staff within an organization

will benefit because the policies clearly identify what is required of them to secure the network, infrastructure and information. Policies provide consistency across the organization and clearly state the position of the company to employees. In addition, a company which officially sanctions and communicates its Security Policies is positioned to handle employee disciplinary issues with respect to unacceptable use or abuse of its computing resources.

METHODOLOGY

We utilize a tested methodology to assessing and developing Security Policies. The methodology has been divided into various phases. A client can choose all or a portion of the phases, depending on its current policy status. The phases and key activities are as follows:

Analysis

Through an interview process, we will identify and review existing security policies and procedures of the organization. We will identify any unique business issues that need consideration during Policy Development. A program owner and the individuals or groups that will participate in the Program Development and approval process will be identified.

Policy Development

We will initially develop and present a draft set of policies that will act as a working document. Through a series of three workshop reviews, a discussion will take place over the content, wording and format of the policies. Based on the discussions, revisions will be made to the document and a set of complete Policies finalized.

Policy Approval

Following the development phase, it is the responsibility of the client to obtain executive approval to have the policies sanctioned as official.

We can provide support, guidance, and assistance during this phase if required.

Employee Awareness

Upon completion of the Security Policies, we will provide recommendations for promoting the policies and security awareness messages.

Security Awareness Program

We offer a Security Awareness Program which is detailed in our Security Awareness brochure. This is the logical next step for organizations that have developed Security Policies.

SUMMARY

We are capable of assessing and writing security policies that are tailored to the specific needs of your business. We also offer a complete package that will include Policy Development and Security Awareness. We can customize the scope and activities in order to meet the needs of your organization, regardless of size.