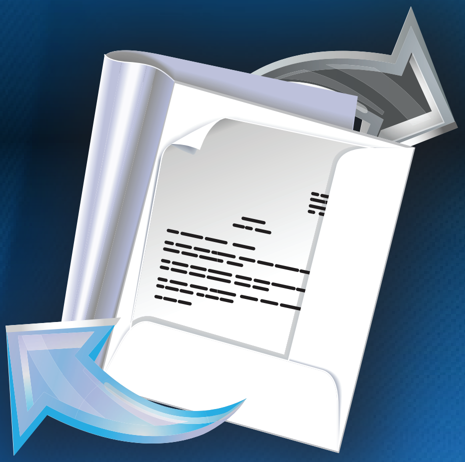
SECURITY 7 NETWORKS

PolicyWerx

IT Security policy development services that reduce corporate risk and protect assets

- Simplifies development of a comprehensive IT security policy tailored to your unique environment
- Ensures compliance with regulations requiring written IT policies, including the Massachusetts data privacy law, PCI DSS and HIPAA
- Reduces business risk by protecting key information technology assets
- Maximizes policy effectiveness by leveraging a knowledge base of proven industry best practices combined with the expertise of skilled security consultants



Protecting Critical Assets and Reducing Risk

Information systems and the associated data have become vital assets for most organizations. They automate mission critical processes, and house crucial information such as customer data, financial records and intellectual property. To safeguard these assets, all organizations need to develop a written corporate IT security policy. The policy should define how IT assets are to be protected, expected employee behaviors and the consequences of violations.

A well crafted security policy not only protects the assets themselves, but also reduces corporate risk. It shields the organization from the financial impact of unnecessary downtime, lawsuits resulting from IT system misuse and the consequences of unauthorized modification or deletion of data. Written security policies are also required by a wide variety of government and industry regulations, including Massachusetts' data privacy law (201 CMR 17), the Payment Card Industry Data Security Standard (PCI DSS) and the federal Health Insurance Portability and Accountability Act (HIPAA), to name a few. Failure to comply with these laws can lead to fines, increased transaction costs and other penalties, which are additional forms of corporate risk.

The Challenges of Internal Development

Most organizations have access to internal IT resources; however they are typically not well suited to the task of developing a corporate IT security policy for a variety of reasons:

- ▶ Internal personnel rarely have policy development experience, requiring them to conduct significant research to identify required topics and articulate appropriate best practices
- ▶ Lack of exposure to the most recent legal, regulatory and technology issues makes it difficult for them to identify and integrate these topics into a policy in any meaningful way without access to outside subject matter experts
- ▶ The policy they develop will not benefit from the substantial experiences of peer organizations, which would help ensure it is effective
- ▶ Writing is typically not a core skill of IT personnel, as a result they may not be in a position to produce the simple, clear, easy-to-read policy required to help ensure adoption
- ▶ A written policy is only one element of a successful program; experience is needed to understand the practical aspects of rolling out and ensuring adoption of the policy across an organization

Policy Development Services to Ensure Results are Achieved Quickly and Cost Effectively

Security7 Networks is an experienced IT services provider which offers a comprehensive security policy development and implementation service. Each engagement begins with an assessment, where our experienced consultants interview your staff to understand your organization, IT environment, practices, risks and business requirements. This information, along with a knowledge base of proven IT policies, is used to rapidly and cost effectively produce a customized security policy that leverages experience gained by building policies for numerous other organizations. A complete policy is delivered electronically in written form, ready to use, utilizing standard RTF format, so it can easily be modified by your internal staff as the policy evolves over time.

SECURITY 7 NETWORKS

PolicyWerx

Industry experience shows that successful adoption of a security policy requires more than just crafting and publishing the policy itself. Security7 Networks brings the practical experience to guide your organization through a more holistic approach; assisting you in considering important factors such as executive sponsorship, training, as well as on-going processes for communication, enforcement and policy modification.

> **"Security7 Networks' experience and knowledge of security best practices, combined with an ability to form a close working relationship with my staff, helped us to quickly implement a corporate security policy which has effectively secured an IT infrastructure vital to keeping our 100 plus facilities operational."**
>
> *John Loftus, CFO, Napoli Group/McDonalds*

A Comprehensive Security Policy Tailored to Your Unique Needs

The corporate IT security policy Security7 Networks delivers will contain a suite of individual policies encompassing the topics important to your particular environment. Appropriate topics will vary depending upon factors such as your organization's size, IT architecture and sensitivity of data handled; however Figure 1 provides an overview of typical subjects covered:

Figure 1: Topics covered in a typical corporate IT security policy from Security7 Networks

Acceptable use of IT assets	Requirements for virtual private network use
Processes to ensure use of secure credentials	Policy regarding local and remote network access
Classification of corporate data to ensure it is appropriately handled	Requirements for IT asset access by 3rd parties, such as outsourcing vendors, suppliers and customers
Storage, use and disclosure of confidential data	IT policy regarding access to resources by corporate guests
Encryption of sensitive data	Employee use of mobile devices
Data retention and destruction policy	Policy to secure corporate email system
Backup processes to ensure data availability	Planned response to an IT security incident
Policy for wireless access to network	Physical security of IT assets

To help ensure successful implementation of your policy Security7 Networks also delivers a variety of operational tools. Typical examples are outlined in Figure 2:

Figure 2: Typical policy implementation tools provided by Security7 Networks

Employee signature form to indicate acknowledgement of policy	Guest and 3rd policy access request forms
Account setup request forms	Notice of policy non-compliance
Request for policy exemption	Security incident form

Identifying and closing security and compliance gaps

In the course of developing your policy, Security7 Networks consultants will note any problematic or missing IT controls suggested by industry best practices. Working with your staff we can help identify the most effective means of closing gaps directly, or through compensating controls. This perspective will help ensure your risks are minimized, and provide the outside view that helps meet the needs of auditors, investors and other corporate governance partners.

An Experienced Managed Services Partner

Founded in 2005 by a team of experienced IT services professionals, privately owned Security7 Networks has profitably grown by providing all its clients levels of service and partnership that are available to only to the top clients of large IT services organizations. For further information on how Security7 Networks can help your organization protect its valuable IT resources and reduce risk using PolicyWerx, please contact us at: **www.security7.net** | **info@security7.net**

- 861 Lafayette Road Unit 4, Hampton, New Hampshire 03842
w: http://www.security7.net - p: (877) 664-9379