

Policies and Practices



ADVISORY
SERVICE

Improve corporate risk reduction with strategic security and privacy services.

Is the Policies and Practices Service right for your company?

- Do you need a cost-effect and comprehensive approach that connects your security strategy through to end-user security awareness and practices?
- Do you have Information Security policies in place that support your organization's mission and goals?
- Do your security policies differentiate you from the competition, and give you a real business advantage?
- What are the legal, regulatory, and contractual obligations for ensuring the security of your data?

Overview

A security policy is an enterprise-wide set of rules of operation to establish measures to protect an organization's information assets. It defines authorization levels; more importantly, it sets out the limits for normal operations. All information, regardless of the industry or size of the company, must be protected and addressed in a security policy. Without these boundaries, there can be no security within an organization.

Digital Defence provides the strategic and technical support needed to evaluate and implement your security policies, processes, and controls. We understand the tradeoffs between cost and security, and can bring an objective view to the policy authoring process, help you to identify any gaps, and support you in creating an Information Security policy that reflects the most effective industry practices and the legal and regulatory requirements.

Using our proprietary process which maps the standards directly to existing and planned business processes, we can highlight the benefits of policy compliance and facilitate its acceptance across an organization.

The Benefits of Having an Established Security Policy and Procedures

Well-written policies are the core of an organization's Information Security strategy. Organization can take advantage of well implemented policies to:

- Ensure that the organization's Information Security objectives are aligned with strategic and business objectives
- Clarify management expectations for the protection of information assets
- Ensure compliance with regulatory and legal expectations; limit liability
- Prepare for security incidents; minimize losses and liability
- Heighten your organization's security awareness and actual practices
- Enhance the organization's image and credibility with employees, customers, and the community

Policies and Standards to Consider

- Strategic information security policy
- Privacy policy for organization and website
- Data classification and handling
- Acceptable use policy (governing employee access to network and data resources)
- Human resources policies pertaining to security and privacy
- E-mail (including webmail), instant messaging policy
- Social networking policies
- Technical policies and standards (firewall, network devices, deployment of servers and workstations, passwords)
- Remote access policy
- Use of personal systems
- Social engineering policy
- Incident response policies

About Digital Defence

Digital Defence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss

When to Review Your Information Security Policy

Because policies are a reflection of your business strategy and practices, they should be reviewed on a periodic basis (usually once per year), and when:

- Potential for monetary loss or embarrassment due to security problems
- Policies have not been reviewed to ensure alignment with strategy, business practices, new technologies, or new business situations (e.g.: merger or acquisition)
- No formal policies are in place, or policies and procedures are used and distributed in an *ad hoc* fashion
- Protection of business information is critical to success
- Ongoing need for employees (internal and external), contractors, and vendors to have broad access to sensitive information
- Assisting in developing and implementing a process for classification of data

Service Description

Digital Defence offers a comprehensive service to ensure that you have the most appropriate Information Security policy and practices in place. Based on your specific requirements, this service includes:

- Security Policy Development—After critically reviewing your business and IT strategy and requirements, Digital Defence will work with you to develop and document your security strategy, policies, and supporting practices
- Security Policy Assessment—Digital Defence will review your existing policies and practices against regulatory requirements, relevant standards, and industry best practices. A gap analysis will be prepared, and policies will be up-dated to address potential weaknesses
- Security Awareness Training—Policies must be delivered to the organization, retained, and practiced in order for them to be effective security controls. Digital Defence will work with you to develop training materials that deliver the message. We can deliver customized training to "train the trainer", or provide training to all employees

For more information please visit www.digitaldefence.ca



Digital Defence Inc

Toll-Free 866-677-1337 | Tel 905-681-3310
302 - 3310 South Service Road,
Burlington, Ontario L7N 3M6

Disclaimer

© 2010 Digital Defence. All rights reserved.
This document is for informational purposes only.
Digital Defence makes no warranties, express or implied, in this document.