# Solution Brief

## Enabling Business with Information Security and Privacy Policies

InformationShield

About Information Shield

Information Shield is a global provider of information security policy, data privacy  and security awareness solutions that enable organizations to effectively comply with international security and privacy regulations.  Information Shield products are used by over 7000 customers in 60 countries worldwide.

Information Shield, Inc.
2660 Bering Dr.
Houston, TX 77057
www.informationshield.com
sales@informationshield.com
P: 888.641.0505
F: 866.304.6704

## Contents

# Information Shield Solution Brief

## *Enabling Business with Information Security and Privacy Policies*

*By David J Lineman*
*Information Shield*

## Summary

*With a dramatic increase in legislation and consumer awareness of identity theft, businesses are finding that security and privacy policies are becoming an essential business tool. In some highly regulated markets, it is difficult to do business at all without a sound set of policies. More than ever, organizations must consider how effective information security and data privacy policies actually enable business.*

*In this overview we discuss various ways that effective, written information security and data privacy policies can actually help increase sales and enable business with key partners.*

Limit of Liability/Disclaimer of Warranty: While the copyright holders, publishers, and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of its contents and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. The advice and strategies contained herein are based on the author’s experience and may not be usable for your situation. You should consult with an information security professional where appropriate. Neither the publishers nor authors shall be liable for any loss of profit or any other commercial damages, including, but not limited to, special, incidental, consequential, or other damages.

## Information Security Budgets Under Pressure

Management at many organizations still views information security as a necessary evil. With a slumping economy, increased competitive pressures and rising business costs, expenses such as information security come under great scrutiny. If it doesn't contribute to the bottom line, then it might be expendable. As always, the internal sales process for information security is an uphill battle. As a part of the overall security program, information security policies often fall to the wayside in tough times. They are deemed to be too complex or too costly to implement.

While businesses are tempted to postpone or ignore their security policy development, the market is creating a different set of priorities. Now more than ever, an organization must consider how effective information security and privacy policies actually enable business. With a dramatic increase in legislation and consumer awareness of identity theft, businesses are finding that security and privacy policies are becoming an essential business tool. In some highly regulated markets such as financial services, it is difficult to do business at all without a sound set of information security and data privacy policies.

## Policies as a Communication Tool

Information security policies serve a variety of critical purposes in the enterprise. First, they are documented business rules for how the organization will protect critical information. Policies form the foundation of the information protection program, establishing the overall information architecture and translating requirements for more detailed standards and procedures. Often overlooked, however, is the role of written policies as a business communication tool both within the organization and with the rest of the business world.

Information security policies provide the written contract between management, employees, and third parties on how the organization will protect information. These third parties include valuable constituents such as customers, business partners and external auditors.

## Policies Enable Business

### Enabling the workforce - Employee Communication

One of the key ways in which policies can enable business is to streamline internal business processes. Security and privacy policies are essential as employees access more sensitive information on more devices in a variety of formats. Ten years ago sensitive customer information may have been confined to a paper folder or a database system. Today, customer information can easily be copied, modified or transmitted electronically in a variety of formats on many different devices. To operate effectively in the modern IT environment, employees must understand their role in identifying and protecting information. In the age of electronic monitoring, employees must also clearly understand how the organization will handle their personal information. A variety of U.S. state-level data protection laws require organizations to protect the sensitive information of employees as well as customers.

## Enabling Sales - Customer Communications

Information security and data privacy policies tell potential and existing customers that their information is valuable and will be protected. As the risk of identity theft grows, consumers and retail customers are looking to see how an organization protects their personal information. A number of studies by the Ponemon Institute [8] indicate that a customer's view of the organization's privacy practices has a dramatic impact on whether the customer chooses to establish and maintain a business relationship. In some cases, a policy on privacy breach notification can become the most critical business policy. Organizations that experience a customer data breach but mishandle the communication process can experience a dramatic loss in sales and repeat customers.

## Enabling Business-to-Business Sales

Within the business-to-business market, the need for security and privacy policies is even greater. Many organizations are finding that they cannot even do business with a large customer without having a comprehensive set of written policies. At Information Shield, we often encounter businesses that after months of effort have finally landed their largest client (possibly a large bank or insurance company), only to find that the entire relationship may be at risk because they do not have written security policies in place. This creates both business and contract delays and can look very unfavorable to larger, more sophisticated clients. On the other hand, a proactive approach to written policies can actually be a competitive differentiator in today's climate.

## Enabling Business Growth – Partner Relationships

Businesses can use security and privacy policies to communicate with business partners. Once again, an increase in regulatory oversight now requires that most businesses validate the security program of any third party that may handle or process sensitive data. (See Table 1)

Organizations that serve the financial industry are used to validation audits such as SAS 70. However, the requirement to validate the security practices of third parties is a key requirement of every information security and privacy-related law at the state and national level. Highly publicized data breaches via third-party mishandling of confidential information is only increasing the pressure from regulators and auditors.

## Enabling Compliance - External Auditors or Regulators

There is hardly a business today that does not fall under some type of data protection or privacy regulation. There are now data protection and privacy laws in over 80 countries worldwide. In the last ten years, a dramatic wave of legislation in the United States created data protection requirements for financial services and healthcare. Now the rampant growth of identity theft and other cyber-crime has driven this protection to nearly any type of personal customer information. For example, as of November 2008 there were forty-four U.S. states that had some type of data breach notification law.

**Table 1: Specific Framework and Regulatory Requirements for Third-Party Security Program Validation**

| Regulation/Standard | Industry | Validation Requirement |
|---|---|---|
| ISO/IEC 17799:2005 | Security Framework | 6.2.1 Identification of risks related to external parties<br>6.2.3 Addressing security in third party agreements |
| HIPAA Security Final Rule (Health Insurance Portability and Accountability Act of 1996) | Healthcare (U.S.) | Business Associate Contracts or Other arrangements 164.314 (a) Contracts must be amended [...] to assure that business partners and agents agree to provide reasonable and appropriate security to protect information (and) (C) Report to the covered entity and security violation of which it becomes aware. |
| Sarbanes-Oxley Act, Section 404 - based on COBIT (Control Objectives for Information Technology – V4.1) | All Publicly Traded Companies (U.S) | DS2 Manage Third-Party Services |
| PCI-DSS Version 1.1 | Credit Card | Requirement 12: Maintain a policy that addresses information security for employees and contractors<br>12.3 Are information security policies reviewed at least once a year and updated as needed? |
| Gramm-Leach-Bliley Act (GLBA) Title V - Section 501 Interagency Guidelines Establishing Standards For Safeguarding Customer Information | Financial Services (U.S.) | Financial institutions are required under the 501(b) guidelines to ensure service providers have implemented adequate security controls to safeguard customer information.<br>- Exercise appropriate due diligence in selecting its service providers;<br>- Require its service providers by contract to implement appropriate measures designed to meet the objectives of the Security Guidelines; and |

Most recently the state of Massachusetts passed 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth. The Massachusetts regulations apply to anyone that owns, licenses, stores or maintains personal information about Massachusetts residents. Massachusetts joins New York, Texas and a growing list of at least thirty 30 states that have data protection requirements in addition to the laws regarding data breach notification.

A growing number of states also have specific laws that require the protection of both employee and customer information. Of course, written security and privacy policies are a key element in these programs.

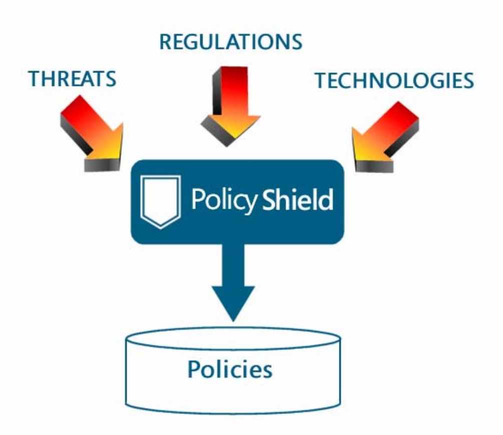
Written security and privacy policies are key pieces of evidence in any legal or regulatory investigation. Poorly implemented or missing policies can increase fines or trigger additional damages. A comprehensive set of security and privacy policies sends a strong message to external auditors that the organization is serious about information security as a key business process.

Auditors, regulators, and federal courts have consistently sent the same message - No organization can claim that it is effectively mitigating risk when it has an incomplete, outdated set of written policies. Written policies form the "blueprint" for the entire information security program, and an effective program must be monitored, reviewed and updated based on a continually changing business environment.

# Cost-Effective Security and Privacy Policies

## Saving Money Building and Maintaining Security Policies

More than ever, organizations are looking for ways to trim costs and streamline business processes. *PolicyShield* is a unique information security policy subscription service based on the "gold standard" policy development guide, *Information Security Policies Made Easy* by Charles Cresson Wood. *PolicyShield* is designed to allow your organization to build and maintain a robust set of written information security policies with the least amount of effort. To achieve this, the PolicyShield library is regularly updated with new policies and resources to help you address new risks.



*PolicyShield* can help address the common resource and organizational challenges to keeping security policies reviewed and updated. For example, *PolicyShield* enhances the productivity of internal staff by dramatically reducing research and development time to develop new policies. PolicyShield resources and templates further reduce the development effort by providing regulatory guidance, tools and checklists.

PolicyShield acts as your "on-demand" security policy consultant. Our team of information security professionals continually monitors the technology landscape to look for new risks to your organization's information assets. These risks may include new threats (such as botnets), regulatory changes (including enforcement actions) and new technologies (instant-messaging, VOIP, etc.)

Security policies within the *PolicyShield* policy library are tied to the ISO 27002 security framework, with convenient mappings to additional regulatory and audit frameworks, helping internal staff build a common set of policy controls that satisfy multiple requirements. This "unified" approach to policy development can save time when coordinating efforts with legal, human resources and compliance efforts.

## About Information Shield

Information Shield has helped over 7000 businesses save time and money building and maintaining written security policies. *Information Security Policies Made Easy*, by Charles Cresson Wood, provides pre-written policies and expert advice covering over 180 separate topics of information security and data privacy. The *PolicyShield Security Policy Subscription* is the next evolution of this leading resource, providing regular updates based on the latest threats, technologies and regulatory changes. In most cases, an organization can save thousands of dollars and hundreds of man-hours building and updating written security policies.

## References and Additional Resources

*[1] Payment Card Industry (PCI) Data Security Standard, Version 1.1* – Published September 2008, PCI Security Standards Council.

*[2] FFIEC IT Examination Handbook - Information Security*, July 2006 - Published by FFIEC. [http://www.ffiec.gov/ffiecinfobase/html_pages/It_01.html]

*[3] ISO/IEC 17799:2005 (ISO 27002) – Code of practice for information security management* - Published by ISO and available at BSI [http://www.bsi-global.org/]

*[4] Control Objectives for Information Technology (COBIT™) 4th Edition* – Published by ISACA, November 2005. [http://www.isaca.org]

*[5] Health Insurance Portability and Accountability Act of 1996 (HIPAA): Final Security Rule.* Department of Health and Human Services; Published in the Federal Registrar. [http://www.hhs.gov/ocr/hipaa]

*[6] NIST Special Publication 800-53, Security Self-Assessment Guide for Information Technology Systems*, November 2008 - Published by the National Institute of Standards and Technology (NIST). [http://www.nist.gov].

*[7] Information Security Policies Made Easy*, by Charles Cresson Wood - Published by Information Shield, Inc. 2005-2008. [http://www.informationshield.com]

*[8] Ponemon Institute 2007 Annual Study: Cost of Data Breach*, Published by the Ponemon Institute. [www.ponemon.org]