Solution Brief

Security Policy Compliance for the MA State Identity Theft Law

InformationShield

About Information Shield

Information Shield is a global provider of 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 59 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

InformationShield

Security Policy Compliance with the MA State Identity Theft Law

By David J Lineman
Information Shield

Contents

1. Introduction

In 2009 the Commonwealth of Massachusetts finalized a law to protect state residents against the growing problem of identify theft. The law sets forth very prescriptive requirements for a written information security program and applies to any organization that stores or processes personal data from a MA state resident. It is likely to impact thousands of organizations. The deadline for compliance with 201 CMR 17.00 is March 1, 2010.

In this paper we outline how organizations can use Information Shield's library of security products to jump-start their compliance efforts. We address each primary section of the law and provide details of our solution maps to the requirements of the law.

2. Written Security Program Requirements

201 CMR 17.03 - "Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards."

Written information security policies are the foundation of any information security program. Information security policies provide the high-level business rules for how an organization will protect information assets. Written policies are also required so that each member of the organization understands their information security responsibilities according to their job role. Written information security policies also provide documented evidence of management's intent to protect information, and a baseline for both internal and external auditors to validate the security posture of the organization.

Like most data protection laws, the rules for 201 CMR 17.00 specify that the program must be "written in one or more readily accessible parts." In short, this implies that every organization must have a set of written information security policies that cover each of the core areas of the regulation. Thus, addressing the primary requirement involves the drafting and maintenance of a comprehensive set of written information security policies and procedures.

Information Shield Policy Development Tools

Information Shield provides a variety of time-saving tools to help organization manage the policy development process and thus address the key requirements of 201 CMR 17. We use the word "process" because policy development is not a one-time project. An effective written information security policy program requires organizations to regularly update policies based on the latest risks to the organization. This implies that organizations must develop a formal process for developing, approving, integrating, and deploying written policies on a regular basis.

Information Shield provided the following time-savings tools:

Policy Statement Library – Information Shield's library of pre-written security policies covers each technical control area in detail, providing flexibility for both small and large organizations. The policy library is organized around the ISO 27002 security framework, and includes over 180 separate information security domains. While our library is based upon the ISO security standard, easy search and browsing facilities make it easy to locate specific written policies related to 201 CMR 17.00. Policy statements can be easily filtered by target audience, security environment (low, medium, high) and keyword.

Policy Implementation Advice - Each policy within the statement library contains valuable commentary to help organizations implement the given policy. The commentary describes the risks that each policy is designed to address, which greatly aids a formal risk-assessment process.

Complete Pre-Written Documents – Our products also contain seventeen complete, pre-written information security policy documents in MS-Word format that address some of the most critical organizational security needs. Examples include access control, electronic mail, internet acceptable use, firewalls, network security, and data privacy.

Policy Mapping Documents – Information Shield products contain high-level mapping documents which provide a guide for locating specific 201 CMR 17.00 security policies. Also included are maps for COBIT 4.0 (used for Sarbanes-Oxley), PCI-DSS and HIPAA [7]. Many organizations are required to demonstrate compliance with more than one regulation or framework. ISPME is designed to facilitate a best-practices approach which allows for audits against multiple standards and regulations.

Detailed Policy Development Project Guidance – Information Shield products contain over 40 pages of expert advice on how to build and develop information security policies. This tutorial is based on the 20 year information security experience of Charles Cresson Wood, CISSP, CISM. The guidance includes helpful checklists to use in the development and deployment of policies.

Valuable Policy Development Forms and Templates – Information Shield products a number of time-saving forms that are required within an effective written policy program. Examples include a Sample Agreement to Comply with Information Security Policies (for all users) and a Sample Risk Assessment Form to process and manage exceptions to policy.

3. Policy Management Program Requirements

Section 17.03 of the law ("Duty to Protect and Standards for Protecting Personal Information") sets forth the management-level requirements of the written security program. From a security management perspective, this section of the law provides more detail of how the written policies will apply to various roles and departments of the organization and how the overall compliance process will be monitoring and updated.

The following table provides a description of how each program requirement area is addressed by Information Shield solutions.

Table 1: Security Program Requirements Addressed by Security Policy

17.03 Duty to Protect and Standards for Protecting Personal Information	
Specific Program Requirements	**Information Shield Policy Solution**
1.0 Protection Requirements *Identification of customer PII requires a data classification program.*	7.2.1 Classification guidelines 7.2.2 Information labeling and handling In order to protect PII is must be classified and labeled. Information Shield provides over 50

17.03 Duty to Protect and Standards for Protecting Personal Information	
Specific Program Requirements	**Information Shield Policy Solution**
	policies for proper data classification.
2. Written Security Program Requirements *Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:*	6.1.1 Management commitment to information security 6.1.2 Information security co-ordination 6.2.2 Addressing security when dealing with customers
(a) Assigned Security Responsibility *(a) Designating one or more employees to maintain the comprehensive information security program;*	6.1.3 Allocation Of Information Security Responsibilities *Information Security Roles and Responsibilities Made Easy* contains a library of over 70 pre-written job descriptions and department-level mission statements. This library enables organizations to quickly document the security responsibilities of over 30 different organizational roles.
(b) Ongoing Risk Assessment *Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:*	6.1.2 Information Security Coordination 6.1.1- 2. Risk Assessments 6.2.1 Identification of risks related to external parties 14.1.2 Business continuity and risk assessment 15.1.1- 6. System Risk Assessments
1. ongoing employee (including temporary and contract employee) training;	8.2.2 Information security awareness, education, and training
2. employee compliance with policies and procedures; and	5.1.1 Information Security Policy Document
3. means for detecting and preventing security system failures.	10.10.2 Monitoring system use
(c) Written Acceptable Use Security Policies *Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.*	5.1.1 Information Security Policy Document 7.1.1 Acceptable Use of Assets Sample Acceptable Use Policy
(d) Employee Sanctions *Imposing disciplinary measures for violations of the comprehensive information security program rules.*	8.2 DURING EMPLOYMENT 8.2.3 Disciplinary process *Agreement to Abide by Security Policies*
(e) Employee termination procedures *Preventing terminated employees from accessing*	8.3.1 Termination responsibilities 8.3.2 Return of assets 8.3.3 Removal of access rights

17.03 Duty to Protect and Standards for Protecting Personal Information	
Specific Program Requirements	**Information Shield Policy Solution**
records containing personal information.	Information Shield's library includes policies for employee termination, including a sample Employment Termination Checklist.
(f) Service Provider Oversight *Oversee service providers, by:*	6.2 EXTERNAL PARTIES Information Shield's library includes over 40 policies for managing the security requirements of third parties.
(f-1)Service Provide Risk Assessment *Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and*	6.2.1 Identification of risks related to external parties
(f-2)Service Provider Contract Requirements *Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information;*	6.2.3 Addressing security in third party agreements
(g) Physical Security Controls *Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.*	9 PHYSICAL AND ENVIRONMENTAL SECURITY 9.1 SECURE AREAS 9.2 EQUIPMENT SECURITY
(h) Security Program Monitoring *Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.*	15.2.1 Compliance with security policies and standards. 15.2.2 Technical compliance checking
(i) Annual Security Program Review *Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.*	6.1.8 Independent review of information security 5.1.2 Review of the information security policy
(j) Incident Response Management *Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of*	13.1.1 Reporting information security events 13.1.2 Reporting security weaknesses Our security policy library contains over 40 specific pre-written policies covering the creation

17.03 Duty to Protect and Standards for Protecting Personal Information	
Specific Program Requirements	**Information Shield Policy Solution**
events and actions taken, if any, to make changes in business practices relating to protection of personal information.	and management of a Computer Emergency Response Team (CERT) as well as the reporting and management of security incidents.

4. Technical Security Policy Controls

17.04 Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

Section 17.04 of the Law sets forth the specific technical security controls that must be in place on computer and communications systems. While the first two sections describe the administrative and management-related policies, this section describes the requirements for technical security controls. While these controls are intended to apply to technology (such as computers and network devices), it is critical these controls are also documented in written policies and procedures.

Addressing Specific Information Security Topics

Information Shield publications include per-written security policies that address each of the technical security requirements of 201 CMR 17.00. The following table maps the specific technical control requirements of MA 201 CMR 17.00 to each specific policy category of our security publications.

Table 2: Specific Security Policy Requirements for 201 CMR 17.00

17.04: Computer System Security Requirements	
Specific Program Objectives	**Information Shield Policy Solution**
1. Identification and Authentication *Secure user authentication protocols including:*	11.2 USER ACCESS MANAGEMENT 11.3 USER RESPONSIBILITIES 11.3.1 Password use. 11.5.1 Secure log-on procedures 11.5.2 User identification and authentication
a. User ID Management *control of user IDs and other identifiers;*	11.2.1 User registration 11.2.2 Privilege management
b. Secure Password Selection *a reasonably secure method of assigning and selecting passwords, or use of unique identifier*	11.2.3 User password management

technologies, such as biometrics or token devices;	
c. Password Protection *control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;*	11.2.3 User password management 11.3.3 Clear desk and clear screen policy
d. User Account Restrictions (expiration) *restricting access to active users and active user accounts only; and*	11.2.4 Review of user access rights
e. Max login attempts *blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;*	11.3.2 Unattended user equipment 11.5 Operating System Access Control
2. Access Controls *Secure access control measures that:*	11 ACCESS CONTROL 11.1.1 Access control policy 11.2 User Access Management 11.4 Network Access Control 11.5 Operating System Access Control 11.6 Application and Information Access Control
a. Privilege Restriction - Need to Know *restrict access to records and files containing personal information to those who need such information to perform their job duties; and*	11.2.2 Privilege management
b. Unique UserID and Passwords *assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;*	11.2.3 User password management 11.3.1 Password use
c. Change Vendor Default Passwords *not vendor supplied default passwords,*	10.3.2 System acceptance
3. Transmission Protection of PII *Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.*	10.7.3 Information handling procedures 10.8.1 Information exchange policies and procedures 10.8.2 Exchange agreements 10.8.3 Physical media in transit 10.8.4 Electronic messaging
4. Systems Monitoring *Reasonable monitoring of systems, for unauthorized use of or access to personal information.*	10.10 MONITORING 10.10.1 Audit logging 10.10.2 Monitoring system use 10.10.3 Protection of log information 10.10.4 Administrator and operator logs 10.10.5 Fault logging
5. Portable Device Encryption *Encryption of all personal information stored on laptops or other portable devices;*	11.7.1 Mobile computing and communications 11.7.2 Teleworking
6. Network Security *For files containing personal information on a system that is connected to the Internet, there must be:*	10.6 NETWORK SECURITY MANAGEMENT 10.6.1 Network controls 10.6.2 Security of network services

6.1 Firewalls *reasonably up-to-date firewall protection and*	11.4.6 Network connection control 11.4.7 Network routing control *(Sample Firewall Policy)*
6.2 Updated OS Patching *[…] operating system security patches, reasonably designed to maintain the integrity of the personal information.*	10.1.2 Change management 12.6.1 Control of technical vulnerabilities
7. Malicious Software Protection *Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions,*	10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE
8. Employee Education and Training *People are a crucial factor in ensuring the security of computer systems and valuable information resources.*	8.2.2 Information security awareness, education, and training

5. MA State Law Security Policies Step-by-Step

A complete set of information security policies for 201 CMR 17.00 can be developed with the help of Information Shield using these four basic steps:

1. **Perform a Gap-Analysis with Current Policies** - A sound first step is to compare your existing security policies against the requirements from 201 CMR 17.00. Use the tables provided in this paper to help define an outline of the requirements for each section of the program. From there, document which of your existing policy documents address these topics.

2. **Prioritize Missing Policies** – The results of Step 1, along with any organizational risk-assessment, can be used to prioritize a list of policy topics that must be covered to enable compliance. This worksheet can be used to track the progress of policies throughout the development lifecycle.

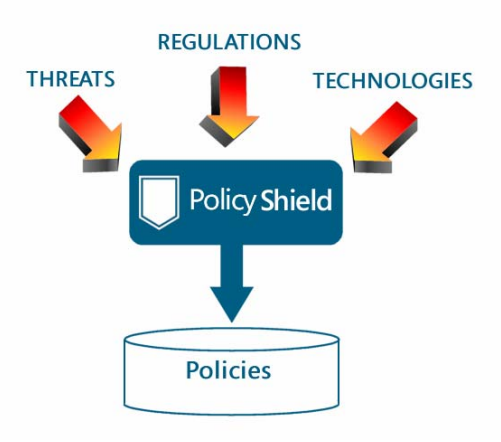
3. **Policy Development and Review Plan** – Use the instructions within ISPME to develop a written information security policy plan. This plan should include, at a minimum, a policy review and exception process, and definition of roles and responsibilities for all members of the organization who may have a role in policy development. Information Security Roles and Responsibilities Made Easy [5] will be a useful tool in the role definition and documentation process.

4. **Build and deploy written policies** – Once the plan has been developed and approved, organizations can beginning developing specific written policies based on existing content within ISPME. ISPME contains fifteen complete sample policy documents that can be used as an excellent starting point. The policy library provides 1400 individual policy statements that can easy be incorporated into existing documents.

6. Staying Up to Date – PolicyShield Policy Subscription

PolicyShield is a unique information security policy subscription service that enables your organization to build and maintain a robust set of written information security policies with the least amount of effort. To achieve this goal, the PolicyShield library is regularly updated with new policies and resources to help you address new risks.

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 risk may include new threats (such as botnets), regulatory changes (including enforcement actions) and new technologies (instant-messaging, VOIP, etc.)



Each quarter we compile a list of new additions to the existing PolicyShield library. New additions may include pre-written information security policies, policy development resources, sample documents, news items and policy-related incidents. PolicyShield is an extremely cost-effective way for an organization to keep written policies up to date and help protect against the latest threats.

Addressing Policy Update Challenges

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.

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.

PolicyShield also helps build a business case for new policies by tying written policies to both real-world incidents and regulatory guidance. By eliminating the time required for research and policy development, internal staff can thus focus on the critical tasks of getting policies approved and integrated.

7. References

[1] 201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH – [http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf]

[2] 201 CMR 17.00 Compliance Checklist – Available from The Office of Consumer Affairs and Business Regulation. [http://www.mass.gov/Eoca/]

[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] *Information Security Policies Made Easy, by Charles Cresson Wood* - Published by Information Shield, Inc. 2010. [http://www.informationshield.com]

[5] *Information Security Roles and Responsibilities Made Easy, by Charles Cresson Wood* - Published by Information Shield, Inc. 2002-2005. [http://www.informationshield.com]

About the Author

David Lineman is President of Information Shield. Mr. Lineman has 20 years of experience in software development, business consulting and information security. He is the author of Information Protection Made Easy – A Guide for Employees and Contractors and is a frequent speaker and author on the subjects of information security policy and regulatory requirements.