InformationShield

Seven Elements of an Effective Information Security Policy Management Program

By David J. Lineman

How mature is your information security policy program? Do you have a set of outdated documents stored in a binder or intranet site? Or do you have a documented management program that keeps your policies up to date, your users informed and your internal auditors sleeping at night?

In this paper we review seven key characteristics of an effective policy management program. These characteristics are culled from leading practices, security and privacy frameworks, and incidents involving information security policies. Organizations can use this quick checklist to evaluate the maturity of their existing management program.

1. Written documents with version control

Even though it seems obvious, nearly every security standard and framework specifically requires information security policies **to be written**. Since policies define management's expectations and stated objectives for protecting information, policies cannot be "implied" – but have to be documented. Having a "written policy document" is the first key control established within the international standard ISO/IEC 1-7799:2005, and is critical to performing both internal and external audits. But what are some characteristics that make for an effectively-written policy document?

Policy documents should be written in plain and simple language. Many information security and privacy policies are written in legalese that is difficult for end users to read and understand. Since user education and training is a key component of all information security frameworks, clear, user-oriented language is critical. If your information security policies are written by either the information technology (IT) or legal department, make

sure you employ a technical writer or other editor who can help simplify the language of your documents.

Policy documents should also have a **standard format** so that they can be effectively managed and updated. The standard format not only enforces consistency among documents, it insures that each document contains key elements that facilitate the overall management of the information security policies, such as the owner/author, title, scope and effective dates of the policy.

Written documents should also have a policy version number. A **policy version number** clearly articulates which version of the policy is in force at the time of publication, and helps maintain a version history of each document. Maintaining a version history is not only good practice for preserving digital evidence in case of a lawsuit, it also demonstrates that the organization was performing due-diligence by updating its security policies on a regular basis.

2. Defined Policy Document Ownership

Each written policy document should have a defined owner or author. This statement of ownership is the tie between the written policies and the acknowledgement of management's responsibility for updating and maintaining information security policies. The author also provides a point of contact if anyone in the organization has a question about specific policies. Many organizations have written information security policies that are so out-of-date that the author is no longer employed by the organization.

Another area of responsibility that can be documented within written policies is the executive sponsor. The executive sponsor is a C-level manager or executive that puts the final "stamp of approval" on each document. A high-level executive sponsor demonstrates to all employees that your organization is serious about information security.

3. Defined Management Structure

To help keep information security policies readable and manageable, it is important to keep the information "level" consistent among the various document types. In other words, it is not advisable to mix policies, procedures, standards and guidelines into your policy documents.

An effective approach is to create a policy governance structure, which breaks information into separate documents for policies, standards and procedures. For example, a Password Policy would state the high-level organizational goals to create and maintain strong passwords. It can refer

to a Password Standard document which defines the detailed controls that make up strong passwords, such as password length, complexity and history. Keeping these structural elements separate allows an organization to update standards and procedures as new technologies or processed are introduced, while updating higher-level policy documents less frequently.

Another high-level management structure is to organization documents into groups based on subject matter. For example, many organizations are managing their information security programs based on ISO 17799:2005. A defined management structure with a naming convention for each category can organize documents by subject matter, allowing easy mapping to various control categories. These same subjects can be the "folders" for organizing documents on an intranet or common server.

4. Target User Groups

Not all information security policies are appropriate for every role in the company. Therefore, written information security policy documents should be targeted to specific audiences with the organization. Ideally, these audiences should align with functional user roles within the organization.

For example, all users might need to review and acknowledge Internet Acceptable Use policies. However, perhaps only a subset of users would be required to read and acknowledge a Mobile Computing Policy that defines the controls required for working at home or on the road. Employees are already faced with information overload. By simply placing every information security policy on the intranet and asking people to read them, you are really asking *no one* to read them.

Policy documents targeted at specific roles also facilitates the use of automated policy document management systems that distribute and track which users have read which policy documents. Some of these automated systems allow organizations to target specific documents to individual or multiple groups within a central directory system, and then keep track of the results according to each group.

5. An Effective Date Range

Written policies should have a defined "effective date" and "expiration" or "review" date. This is critical so that individuals and organizations know when they are subject to the rules outlined in the policy, and when they can expect updates. The effective dates within your policies should match the organization's written objectives with regard to updating policies. For example, if written policies are to be reviewed at least annually, the effective date and review data should obviously be a year apart. As each policy comes up for review, the document owner (mentioned above) will review the

document for possible updates. Once reviewed, the document can again be published with a new effective date and review date.

Version control and effective policy dates are necessary if the organization is going to successfully apply sanctions to individuals who may violate the policy. For example, if you don't know which version of the Internet Acceptable Use policy restricted the use of personal instant messaging, how can you sanction anyone for violating the policy? Many users who were terminated for violating a company policy have successfully defended themselves by pleading ignorant when the company who fired them had a haphazard set of old, incomplete, and out-of-date policies. A regularly updated set of policies is another indication of management support.

6. A Verified Audit Trail

Policy documents will not be effective unless they are read and understood by all members of the target audience intended for each document. For some documents, such as Acceptable Use or Code of Conduct, the target audience is likely the entire organization. Each policy document should have a corresponding "audit trail" that shows which users have read and acknowledged the document, including the date of acknowledgement. This audit trail should reference the specific version of the policy, to record which policies were being enforced during which time periods.

For smaller organizations, this audit trail can be a simple manila folder with signature pages. For large organizations, automated policy management tools allow for audit logs to be built automatically as users interact with the policy documents via a secure intranet site. In any case, your goal is to be able to verify that each and every person handling information within your organization has read and understood the security policies that apply to them.

Pay special attention to privacy laws when compiling audit logs of any user actions within your organization. Be careful not to collect and save unnecessary sensitive personal information about the user. In some EU countries, such as Germany, even collecting basic log data on user activities is considered a violation of privacy.

7. A Written Exception Process

It may be impossible for every part of the organization to follow all of the information security policies at all times. This is especially true if policies are developed by the legal or information security department without input from business units. Rather than assuming there will be no exceptions to policy, it is preferable to have a documented process for requesting and approving exceptions to policy. Written exception requests should require the approval

of one or more managers within the organization, and have a defined time-frame (six months to a year) after which the exceptions will be reviewed again.

Policy exceptions can be managed within the same framework as the policy documents themselves. In other words, exception should be documented, have a clear owner, and can be organized by topic area.

Automated Solutions

For large organizations, following a standard of due-care for managing information security policies is a time-consuming task. The basic process of recording which of your hundreds or thousands of employees have read even *one* of your policy documents may consume many man-hours. Fortunately, automated policy management tools, such as the VigilEnt Policy Center (VPC) allow organizations to effectively management their written policy documents with a minimum of manpower.

An automated policy document management tool helps facilitate each of the seven characteristics. A set of robust document management features allows for easy editing, update and version control, with centralized review and publishing of documents. Role-based access control assures that only select individuals can review and approve policies for publications. Documents are given a specific window of availability that can match the effective date written on the policy. These and other customized attributes allow for very effective targeting of documents.

Within most automated tools, users are given access to a custom intranet portal that gives them access to the documents which apply to them, based on their role. More robust policy tools also allow for quizzing features to test a user's comprehension of each policy document that have been required to read. Acknowledgement via digital-signatures allows the organization to easily record the date and time each document was read be each user.

Some products, such as VPC, allow organizations to integrate the policy "portal" into their existing LDAP-based or Windows directory structure. This integration allows easy targeting of documents based on a user's group membership. Management reports can then be run on a regular or ad-hoc basis to determine the overall compliance level at the group or organizational level.

About VigilEnt Policy Center

VigilEnt Policy Center is one of the leading policy management systems available. Introduced in 1999 and now on its fourth version, VPC was the

first intranet-based policy management tool on the market. For more information on VigilEnt Policy Center, visit the Information Shield web site at http://www.informationsheild.com/vpc_main.html.

VigilEnt Policy Center ™ is a registered trademark of NetIQ/Attachmate. Information Shield is an authorized reseller of the VPC product.

About Information Shield

Information Shield is a global provider of security policy 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. Find out more at www.informationshield.com or contact us at sales@informationshield.com.

informationshield.com
2660 Bering Drive Houston, TX 77057 TEL 1.888.641.0500 FAX 713.783.5365