Developing a Security Policy

An Enterprise Security Policy Management Framework – Part 2

By Mark Simon – in Collaboration with Microsoft’s Trustworthy Computing Group

Microsoft recognizes the importance of information security policies and how, as business rules, they are necessary for preserving the confidentiality, integrity and availability of information. The information security policy management framework described in this article is part of Microsoft’s Prescriptive Guidance and Education effort, helping management meet its fiduciary obligations in addressing information security. It is technology agnostic and draws upon many industry-accepted standards for managing security risk. It is an important example of Microsoft’s commitment to delivering quality guidance to help customers secure their Information Technology (IT) infrastructures. This information incorporates real-world experiences from Microsoft IT, industry standards and includes input from Microsoft partners.

Guidelines for drafting security policies

This is the second of a two-part series addressing the development of an enterprise information security policy management framework. The first part discussed (a) the function security policies serve in an information security management system and (b) elements of an effective information security policy development program. We will now look at (c) guidelines for drafting successful information security policies, (d) post-development considerations, and (e) enterprise-level information security policy topics that warrant attention.

Issue-specific and system-specific policies

A myriad of events may spur the development or reassessment of issue-specific and system-specific information security policies. A policy could be developed as part of an information security plan. New threats or technologies, an information security incident or a vulnerability assessment could be an impetus to information security policy development. Other factors that may drive a policy change are new risks owing to the acquisition or development of new business units, outsourcing, organization downsizing, and changed legal requirements. Finally, some organizations schedule periodic reviews of their information security policies in an attempt to mitigate these concerns.

Adopting the procedures listed below will contribute to well-formulated information security policies.

1. Project leader or policy development group identifies need to develop or reassess a policy
2. Perform a risk assessment to determine the security needs – see Microsoft’s Security Risk Management Guide which describes how to go about the risk assessment process, including gathering data, prioritizing risks and defining threats and vulnerabilities
3. In light of the risk assessment and the identified need for a new or modified policy, the policy development group determines the policy security objective(s)
4. Stakeholders are consulted on the policy information security objectives, scope, assigned responsibilities, and implementation issues, which leads to the formulation of the policy as well as to the identification of any standard, procedure, guideline or other security control that may be necessary for implementation of the policy
5. Identify the policy scope, including the persons who will receive the policy

6. Identify who must approve the policy and all necessary reviewers
7. Draft the policy
8. Obtain stakeholder feedback
9. Revise the policy as necessary in response to stakeholder comments
10. Submit the policy for approval by management
11. Determine the document’s classification, e.g., public, internal use, confidential
12. Prepare an implementation plan
13. Issue policy and proceed with implementation plan

Figure 4 illustrates the sequencing of the above steps.

Choose enforceable rules

All persons having access to organizational information assets require clarity in their day-to-day activities in managing their use of those assets. To be effective in driving responsibility and risk management for information assets into the organizational culture, organizations need to provide explicit direction about what behavior is acceptable and what behavior will be penalized. As with all quality and improvement programs, the way in which a company treats enforcement of its information security policies will be one, if not the most important, way of ensuring that its security risks and mitigating controls are taken seriously. Without enforcement, an information security policy is reduced to a mere suggestion or guideline.

Manage security policy exceptions

It is inevitable in any information security policy program that unusual events or transactions will arise. Exceptions to information security policies should be permissible where a risk assessment justifies non-compliance. A process should exist for identifying policy exceptions and escalating exception approval to the individual(s) who is (are) responsible for the policy and information assets involved. The process should include documentation of the exception requested, the basis for the request, and management’s approval of the request. Management should be expected to approve an exception to an information security policy when the facts and circumstances warrant an exception. An information security policy could have its own exception approval process or it could be subject to a general policy on information security policy exceptions.

Target the audience

The key to changing behaviors that may compromise information security is to target the relevant audience whose behaviors or responsibilities are at issue. Keeping policies prop-

Corporate Security Policy Development Process

Without enforcement, an information security policy is reduced to a mere suggestion or guideline.
erly targeted on a need-to-know basis enhances perceived importance and relevance of the policies, and makes more reasonable the scope of each person’s policy compliance effort. Knowing the intended audience for a policy is also important to (a) budgeting for implementation resources, (b) choosing policy distribution channels, (c) determining the scope of security policy awareness and education training, (d) and ascertaining the degree of confidentiality that the policy may require.

Policy metadata
Policy development, implementation, and maintenance can be made easier by using policy metadata. The following is a list of policy metadata that an organization may find useful:

- Approved by
- Author
- Classification – public, internal use only, or highly confidential
- Contact information
- Cross references to other policies
- Date – approval date, effective date, revision date, last scheduled review date and next scheduled review date
- Digital fingerprint
- Distribution lists – development, approval and implementation
- Document type – working draft, final, or revision
- Information rights management settings – copying, printing, editing, distribution, password protected
- Location – URL or physical location where the policy can be accessed
- Number of pages
- Policy custodian
- Policy reference number
- Policy subject
- Policy title
- Sources used
- Status – pending, approved, superseded, or rejected

Policy template
An information security policy template makes the development process more efficient by decomposing policies into manageable parts. In addition to the metadata described above, a security policy template ordinarily includes the following elements:

- **Policy heading** – Contains metadata such as the policy title, effective date, reference number and identification of the person who approved the policy.

- **Objectives** – Describes what the policy is attempting to achieve. The effectiveness of the controls that implement the policy will be determined by how well the objectives are met.

- **Audience** (Scope) – Describes to whom the policy is intended to apply. Policies may be aimed at users who fulfill a particular job function, user application roles, users and administrators of specific systems, and external parties.
• **Keyword definitions** – Provides a glossary to facilitate the understanding of technical or business terminology used within the policy statement.

• **Policy statement** – Provides the specifics of the policy message or rules. It should define what actions or behaviors are required or prohibited.

• **References** – Other documentation may be referenced in support of the policy statement such as related policies, standards, guidelines or procedures.

• **Exceptions** – This section should appear unless a general policy on exceptions applies. Policy exceptions recognize that information security ultimately must support the business mission and objectives, but management may be called upon to approve exceptions. Requirements for documenting a policy exception and recording the risk management issues that warrant a policy exception can be addressed here.

• **Enforcement** – This section should appear unless a general policy on enforcement applies. Typically, this section provides information on management’s role in addressing policy violations and specifies possible sanctions such as:
  - Suspension or termination of access
  - Disciplinary action up to and including termination of employment
  - Civil or criminal penalties

### Post-development considerations

#### Policy implementation issues

- The development of implementing standards, guidelines and procedures may be concurrent with the policy development or follow policy issuance. As the security environment changes, implementing standards, procedures and guidelines may be modified as necessary, but the overarching policy may remain constant.

- **Policy distribution** – Web technologies are increasingly the means of choice for distributing information security policies. Web-based policies are inexpensive to deploy, may integrate with existing access controls for web applications, and facilitate cross-referencing and keyword search functionality.

- **Awareness raising methods** – There are a myriad of methods for raising information security policy awareness. Choice of an awareness raising method should reflect the targeted policy audience, and the complexity of the policy and the related standards, procedures or guidelines upon which policy implementation is based. Channels of policy communication include personal interactions (e.g., policy training sessions, new employee orientation meetings, and audits), written materials (e.g., employee acknowledgement statements, contracts with third parties, articles, and brochures), system resources (intranet web sites, logon banners, and automated surveys and questionnaires) and audio-visual materials. In-depth coverage of security awareness delivery methods and techniques is provided in Microsoft’s *Security Awareness Toolkit and Guide.*

#### Assessing policy implementation effectiveness

The cause and effect relationship between a policy and the behavior it may require or proscribe is dependent on the effectiveness of the controls used for the policy’s implementation. Suppose, for example, an organization promulgates an acceptable use policy that restricts employee Internet use to business activities. Notwithstanding the acceptable use policy, Internet activity logs reflect no discernable reduction in employee time spent accessing auction, e-retailing, and gaming sites. While the expression of the acceptable policy may be perfectly fine, it is apparent the controls that implement the policy are not. In this case, insufficient resources may have been devoted to security awareness training, Internet filtering software may not working properly, or there may be poor coordination between Internet usage monitoring and enforcement of the acceptable use policy.

Policy implementation effectiveness can be determined by a variety of factors, including but not limited to self-assessment, the internal audit process, an information security incident, or a vulnerability assessment. The development and selection of specific metrics to measure the impact of security controls is beyond the scope of this article. Guidance on this topic may be found in NIST Special Publication 800-55 Revision 1 (Draft), “Security Metrics Guide for Information Technology Systems.”

#### Policy maintenance and review

A myriad of events may spur the reassessment of information security policies. A policy could be developed as part of an information security plan. New threats or technologies, an information security incident or a vulnerability assessment could be an impetus to information security policy development. Other factors that may drive a policy change are new risks owing to the acquisition or development of new business units, outsourcing, organization downsizing, and changed legal requirements. Finally, some organizations schedule periodic reviews of their information security policies in an attempt to mitigate these concerns.

Management of policy changes should follow a prescribed process where responsibilities and procedures for policy changes are defined. Microsoft addresses change management in-depth in *Change Management,* part of Microsoft’s series on articles on service management functions.

---


Summary
This Enterprise Security Policy Management Framework addresses (a) the function security policies serve in an information security management system, (b) elements of an effective security policy development program (see Part 1, the ISSA Journal, February 2008), (c) guidelines for drafting successful security policies, (d) post-development considerations, and (e) enterprise-level security policy topics that warrant attention.

Information security policy maintenance and review policy mark the end of the information security policy life cycle. To review, this information security policy management framework addresses the following aspects of the information security policy lifecycle, illustrated in Figure 5 below.

Among the most important aspects of this Enterprise Security Policy Management Framework are the following:

- **Making clear the intent or objectives of a policy** – Common objectives are to acquaint personnel with information security risks and the expected ways to address those risks, to clarify responsibility with respect to the protection of information system assets, or to enable appropriate decisions about information security.

- **Demonstrating senior management buy-in** – Management’s support for information security policy development, implementation efforts, compliance monitoring and enforcement is essential to the successful use of information security policies. Management’s commitment and support for information security policies can be demonstrated by the allocation of sufficient resources for policy development and implementation, holding the organization accountable for enforcement and compliance with approved policies, and by management’s participation in the policy approval process.

- **Limiting complexity** – Information security policies should use well-defined terms, succinct language, and clear direction at to what is required or prohibited to help make policies more understandable.

- **Communication** – People need to be made aware policies exist and of their responsibility for compliance. There are a variety of ways to reinforce knowledge of information security policies. Make access to security policies readily available to those who need to know them. Provide information security awareness training and motivate people to take responsibility for information security. Conduct information security risk assessments and engage users in the assessment process. Conduct audits and check for compliance. Hold meetings to discuss vulnerabilities and what can be done about them. Survey internal and external users to determine what they think of the state of security. Publish security articles for organizational communication channels such as newsletters, intranets and extranets. Have users acknowledge their receipt and understanding of security policies in writing.

- **Maintaining relevance** – Information security policies need to keep up with organizational changes, technology, emerging threats, and legal requirements. Security policies should be periodically reviewed or as often as change drivers require.

- **Applying fair and consistent enforcement** – Non-compliance undermines the usefulness of information security policies. A process should be in place so that non-compliance is addressed in a consistent manner.

Management is more likely to achieve its information security policy objectives by following this framework guidance. Use of this framework should be scaled to information security policy development methods and procedures reflective of the risks to information assets as particular facts and circumstances warrant.

About the Author
Mark S. Simon, an attorney in Chicago, Illinois, is Director of Regulatory Compliance Consulting at Eclipsecurity, LLC, and adjunct faculty at DePaul University School of Computer Science, Telecommunications and Information Systems. At Eclipsecurity he specializes in incident response planning, privacy assessments, and regulatory compliance. At DePaul University he instructs a graduate level course on legal aspects of information assurance, and at the undergraduate level he has taught incident response and computer forensics. He holds the Certified Public Accountant certificate, obtained his Juris Doctor and Masters in E-Commerce Technology degrees from DePaul University. He may be reached at msimon@eclipsec.com.