Security-Policy Style

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

Why Does Style Matter?

One of the major areas of my work and operations management has been the development and refinement of information-security policies. Over the years, I have seen cases in which well designed policies have been implemented in effectively in part because of style of presentation. Style is defined in the Encarta Dictionary as a "way of writing or performing: the way in which something is written or performed, as distinct from its content." Style includes the wording and tone, organization, presentation, and even maintenance of the policies. Style influences the reception and effectiveness of policies.

Writing the Policies

Policies should include both prescriptive and proscriptive content; that is, the policy should describe both what people should do and what people should not do in clear, definite, and unambiguous style. Policy writers should aim for short, simple declarative sentences rather than long, complex, meandering sentences. Every policy should include a simple explanation of its purpose; additional explanations in more depth should be available as optional hyperlinks. Policy handbooks should include several ways of locating specific policies; e.g., detailed table of contents, multilevel headings throughout the text, and extensive indexes.

Organizing the Policies

Policies should be made available in multiple formats. The topical organization presents policies in a sequence corresponding to an overall conception of security goals. For example, one can organize security policies starting at the external perimeter (physical security issues such as facilities protection, employee identification and authentication for physical access, and loss-prevention policies) and work inwards.

Special-purpose documents focusing on the security needs of particular groups are another view of the security policies. It is pointless to provide secretarial pool with policies defining internal firewall policies; it's a waste of time to inflict details of separation of duty in accounting functions on the helpdesk staff. Security policy documents should be useful and relevant to the groups for which they are compiled.

All the policies should be structured hierarchically; i.e., they should start with a general description and present increasing detail at lower levels of the policy document. For example, the security-policy section of Charles Cresson Wood's *Information Security Policies Made Easy* < http://www.informationshield.com/ispmemain.htm > (Section 3 in the 10th Edition) starts with the following topics:

1 Information security policy document

1.1 Information protection
1.2 Use of information
1.3 Information handling, access and usage
1.4 Data and program damage disclaimers
1.5 Legal conflicts
1.6 Exception to policies
1.7 Policy non-enforcement
1.8 Violation of law
1.9 Revocation of access privileges
1.10 Industry-specific information security standards
1.11 Policy-driven information system security architecture
2 Review and evaluation
2.1 Security controls enforceability

Presenting the Policies

Two decades ago, most of the organizations I worked with used paper documents for their policies. Typically, employees would receive huge loose-leaf binders for the policies; some organizations also used short paper documents for specific purposes and even reference cards, summary sheets, stickers and posters to communicate their policies. Updating this material was a nightmare: one would often see the security binder topped with stacks of unopened envelopes containing quarterly updates that employees were supposed to manually insert into their binders to replace outmoded policies and include new ones. There's nothing wrong with providing cute, clever reminder cards or attractive posters reminding people of security policies as part of a security awareness campaign; however, expecting employees to maintain paper versions of policies that most see as secondary to their work is unrealistic.

Electronic versions of policies are far more effective in my opinion than any paper compilation can be. In addition, electronic policies offer hypertext, whether in HTML or XML, RTF and word-processor files, or PDFs and HELP files. Links allow users to find material quickly, reducing irritation and frustration when looking for specific policies.

Maintaining the Policies

I strongly recommend that every organization commit to continuous process improvement. For security policies, it should be easy for employees to suggest improvements in any aspect of policies. A committee that includes representatives from throughout the organization should meet periodically to consider those suggestions an update the policies as appropriate. The proposed changes should be circulated as draft for input; such exposure can contribute to a legitimate sense of policy ownership for employees. Major changes should be announced by upper management with an emphasis on explanations of those changes. If the policies are always available online rather than being printed, the changes will be instantly visible.

Class notes on Chapter 44, “Security Policy Guidelines,” from the *Computer Security Handbook*, 5th edition< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ >, are freely available in PPTX< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch44_security_policy_guidelines.pptx > and PDF< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch44_security_policy_guidelines.pdf >.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *