

Chapter 5
Policy Development for Information Security

Mark Bruhn and Rodney Petersen

Computer and Network Security
in Higher Education

Mark Luker and Rodney Petersen, Editors

A Publication of EDUCAUSE

Copyright 2003 Jossey-Bass Inc.

Published by Jossey-Bass, A Wiley Company. Reprinted by permission of John Wiley & Sons, Inc. For personal use only. Not for distribution.

Policy Development for Information Security

Mark Bruhn and Rodney Petersen

Successful efforts to improve security on various campuses have not followed a single formula. In some cases, it took a serious security incident to capture the attention of senior management and provide the impetus for change. In other cases, the leadership and support of the chief information officer or another senior official was the critical factor. Although common ingredients can be found, the experiences of colleges and universities across the country suggest there have been multiple paths taken and varying paces at which institutions are working to meet their security goals.

This chapter describes the importance of policy development for information security and different ways within a college or university setting to get the desired results.

Security Strategies and Plans

A common plea among many IT staff and data stewards revolves around development of an “information security policy” for the institution. Initially, these constituents are not expecting or demanding the kind of detailed institutional policies and procedures described later in this chapter. Rather, they desire some demonstration of a commitment on the part of the senior administration to a program of improved information security. Indeed, a helpful security policy might take the form of a statement of strategic direction or symbolic

expression of organizational value accorded to an information security program. This approach is consistent with general policy processes, inasmuch as policies are often (and, if not, should be) validated by strategies or plans established or endorsed by executives and other institutional decision makers. Such a statement related to IT security needs only to identify improving security of the technology environment as a priority and demonstrate a corresponding commitment by directing or encouraging allocation of the necessary institutional resources. The statement does not need to be—and should not be—clouded by mechanical details designed to dictate technologies that must be employed and standards that must be followed. Those standards should be set later and be supported by the policy statement.

The vision for any information security program should be to support the attainment of institutional goals and priorities. It is easy to sometimes confuse security as the end goal instead of as an activity among many others that supports the purposes for which the enterprise exists—teaching and learning, research and discovery, and outreach and service. The goals of an information security program are to ensure the confidentiality, integrity, and availability of information and organizational resources. Information security, like technology in general, must be approached as an enabler of institutional processes and a means to support attainment of the broader mission.

Security Policies and Procedures

Although there is a close relationship between “plans” and “policies” as described in the previous section, a strategic or tactical plan is not a substitute for a formal statement of institutional intention or direction that is typically contained within a formal institutional policy. The term *policy* can mean different things to different people. As used in the previous section, it can represent the strategic direction or operating philosophy of an organization. *Policy* is also

a term used to describe legislative and regulatory developments, also known as *public policy*. However, in the context of operational statements or directions, colleges and universities tend to think in terms of *institutional policies*. This section outlines elements of institutional policies and other supporting documents, describes an effective policy development process, reviews some sample security policy issues, and explores the model set of authorities for information security at Indiana University (IU).

Elements of Institutional Policies

If the goal of institutional policies is to direct individual behavior and guide institutional decisions, then the effectiveness of formal policy statements will depend on their readability and usefulness. Many colleges and universities suffer from the lack of a common and consistent approach or format for writing organizational policies. Policy development is often confused and sometimes derailed because of the misunderstanding or misuse of terms with important meanings to a professional policy administrator, legal counsel, and others. The outline below suggests some common elements.

Rationale or Purpose

The rationale or purpose statement expresses why the policy is being written. The rationale or purpose may also contain or cross-reference “background” materials or more explanatory details regarding legal, regulatory, or other factors that led to the development of the policy.

Policy Statement

The policy statement should be a concise statement of what the policy is intended to accomplish. The policy should only be a one- or two-sentence description of general organizational intent with respect to the specific topic of the policy. The policy statement should be general enough to provide some flexibility to accommodate new circumstances or periodic changes in technology. Policies

are statements that reflect the philosophies, attitudes, or values of an organization related to a specific issue. Procedures, guidelines, checklists, and standards all must implement, reflect, and support the applicable policy or policies.

Scope of Policy

The scope of the policy can set important parameters such as to whom the policy will apply (for example, faculty, staff, students, and guests) and to what (for example, paper and electronic records, information and computer assets).

Procedures

The procedures detail how the policy statement will be accomplished. Procedures contain one or more sentences describing how to accomplish a task or reach a goal. The specified actions are generally mandatory for the specific situation. More explanatory text is usually involved. A sequence is not necessary but sometimes is important. Procedures may include information on how to report computer security incidents. Procedures may also describe enforcement provisions or methods for appeal.

Roles and Responsibilities

The procedures may contain details about who is responsible for what. The policy should also identify who is responsible for enforcement or compliance and who will provide interpretations in the event of the need for clarification or when there is a dispute.

Definitions

Policies should be precise and easy to understand. Sometimes terms will need to be defined to clarify meaning. However, the policy should attempt to convey messages in simple yet precise terms; excessive definitions may make a policy document unreadable or subject to greater scrutiny when a particular term critical to a dispute is left undefined.

References

Other existing policies or organizational documents might exist that complement, supplement, or help explain the provisions contained within the current policy. References to other policies, guidelines, checklists, standards, organizational documents, and citations to statutory or regulatory items can improve the usefulness of the policy.

Guidelines

Guidelines contain information about how to accomplish some task or reach a specific goal. They are provided as suggestions; in other words, they are not mandatory, but they are a good idea. That is, they represent “best practices” and, although alternate actions might be available and might work, those being provided have proven to be the fastest, cheapest, and so on.

Checklists

Checklists contain one or more statements dictating how to accomplish a task, that is, “commands.” The items are applicable to an immediate circumstance and mandatory in that defined situation. Checklists are typically immediately at hand and written in simple language with no amplifying text. The sequence is always important. Flowcharts are also used as a method for conveying similar information.

Standards

Standards are statements dictating the state of affairs or action in a particular circumstance. They establish a rule from a recognized authority, with no deviation allowed.

Several helpful books and resources are available that describe typical security policy elements and include sample statements for security that correspond with the areas identified above (Barman, 2002; Desman, 2002; Joint Information Systems Committee, 2001; King and others, 2001; Nichols, Ryan, and Ryan, 2000; Peltier, 2001,

2002; Tudor, 2001; U.S. Department of Education, 1998; Walker and Cavanaugh, 1998; Wood, 2002).

Policy Process

Some institutions have developed a “policy on policies” that provides an institutional statement and set of procedures about the elements of institutional policies, who develops them, and how they get approved (see “Formulation and Issuance of Policies” from Cornell University at www.univco.cornell.edu/policy/pop.for.html and “Guide to Writing University Policy” from the University of Minnesota at www.fpd.finop.umn.edu/groups/ppd/documents/information/Guide_to_Writing.cfm). The benefit of a formal approach is that it makes policy development consistent and recognizes policy approval authorities.

The Association of College and University Policy Administrators (ACUPA) promotes a document entitled Policy Development Process with Best Practices (2001) that contains the following stages: (1) identify issues, (2) conduct analysis, (3) draft language, (4) get approvals, (5) determine distribution/education, (6) solicit evaluation and review, and (7) plan measurement and compliance. Stages 1 and 2 are considered “predevelopment,” whereas stages 3 through 5 are part of “development” and stages 6 and 7 are “maintenance.”

The process recommended by ACUPA contains several useful features for the development of security policies. First, issue identification as a proactive component should build on a security risk analysis as discussed in Chapter Three of this book, including the identification of existing information or data security policies.

Second, the identification of the policy owner, policy path, and policy development team is critical to ensuring the ultimate success of the security policy. Views are mixed about whether or not to include legal counsel as part of the drafting team or whether legal counsel should only be a part of a subsequent review process to determine the legal sufficiency of policy documents. Allowing legal counsel to work with the policy early on leads to the possible dan-

ger that a security policy will be written in terms too complex for its intended audience. However, lawyers should be knowledgeable about security requirements under federal or state law.

Third, drafting language and getting approvals is a strategic and political process at most institutions. Because of the urgency of computer and network security for our institutions, it may be more expedient to issue “guidelines” or “interim policies and procedures” to protect assets and ensure legal compliance while using shared governance processes for formal review and adoption of institutional policy.

Fourth, education and awareness of security issues and the corresponding policies and procedures is critical. A policy that no one knows about or a policy that is not followed can do more harm than good.

Finally, the maintenance stage underscores the importance of regularly evaluating security policies to ensure that they are effective and evolve as vulnerabilities change and technology evolves.

Security Policy Issues

Writing “the” security policy to cover all of the possible issues and considerations is an often intimidating and formidable task. It should come as no surprise that security policies come in every shape and size depending on the complexity of the organization, pressing requirements for legal and regulatory compliance, or resources available to devote to policy development. Although there is a tendency to want a “template” or model policy to follow, there is recognition that policies must be designed to meet the needs of the affected communities, while keeping an eye on the importance of education and awareness of the resulting policy elements. Yet there is a need for a broad understanding of the policy issues to be addressed and at the same time a need to access a robust collection of policies and policy development resources on which to draw. For the latter, the reader is referred to the EDUCAUSE/Internet2 Computer and Network Security Task Force Web site (www.educause.edu/security) and the

SANS Security Policy Project Web site (www.sans.org/resources/policies) as two excellent sources of policy collections and related resources on IT security policy issues. Comprehensive outlines of what to include in a security policy are available at www.sans.org/rr/policy/policy.php (Farnsworth, 2000) and www.boran.com/security/IT1x-6.html ("IT Security Cookbook," 2000).

Acceptable Use Policy

Colleges and universities have generally addressed computer security issues through their acceptable use policies. A typical acceptable use policy contains provisions about unauthorized access to computer systems and files, the need to safeguard user IDs and passwords, what levels of privacy to expect, and general prohibitions regarding illegal activities, including computer crimes. It is possible to modify an existing acceptable use policy to include additional responsibilities for security not previously included. However, acceptable use policies are targeted toward end users of computer systems and establish parameters for appropriate use of computing resources. They are considered a "component of the overall information security policy" (Mandia and Prosis, 2001, p. 463). They do not typically stress how users, technology staff, and departments have to behave in order to secure systems, nor do they provide guidance on security practices or how to best maintain systems.

Other Policy Issues

A number of specific policy issues touch on computer and network security. A comprehensive security policy might attempt to address as many as possible of the topics listed below in one collective document (see the security guide for San Francisco State University Division of Information Technology at www.sfsu.edu/~helpdesk/docs/rules/security.htm) or attempt to chip away at each topic individually in support of broader policy objectives (see the departmental security contact policy for the University of California, Berkeley, at socrates.berkeley.edu:2002/contacts.html). In any

event, institutions should review their policies, procedures, and practices to see whether the following topics are addressed:

- Audits and risk assessments
- Authentication and enterprise directory
- Authorization and access management
- Backups and disaster recovery
- Business continuity
- Computer disposal and disk wiping
- Confidentiality and nondisclosure
- Configuration standards for desktop computers
- Departmental security contacts
- Domain name system service
- Encryption, public key infrastructure, and private key escrow
- Filtering and intrusion detection
- Firewall implementation
- Hardware and software asset inventory
- Incident classification and reporting
- Incident response team and protocols
- Laptops and portable equipment security
- Logging and monitoring practices
- Password protection
- Physical access to data centers and other critical sites

- Physical security of equipment
- Privacy of personal information
- Privacy of user files and content
- Remote access to systems and resources
- Responding to law enforcement requests
- Safeguarding financial information
- Scanning for vulnerabilities
- Software licensing and compliance
- Supervision and training of staff
- Virtual private networks
- Virus prevention and detection
- Wireless communication

Examples of policies or further description of the security issues identified above are available from the EDUCAUSE/Internet2 Computer and Network Security Task Force (www.educause.edu/security) or SANS (www.sans.org/resources/policies) policy Web sites.

Model Authority for Information Security

A well-publicized data exposure incident involving Indiana University's bursar's office in February 2001 shed light on the fact that a concerted effort between university departments and the central IT policy and security staff is necessary to ensure that all aspects are considered in responding to an incident. During this particular incident, the common complaint by affected individuals—and the aspect of most interest to the media—was that the length of time it took to notify the potentially affected individuals was

too long—letters were sent twenty-five days after the exposure was recognized.

During the annual report on the state of security from the vice president for information technology and CIO (VPIT/CIO) to the IU Board of Trustees in May 2001, detailed information about the cause and the response to the bursar's office incident was presented. The presentation also included information about the likely lack of preparedness of IU departments to prevent similar incidents and their capability to react appropriately should other incidents occur. Although some in the IU community suggested that the VPIT/CIO had the implied authority to take steps to improve IT security across all departments and campuses and to become directly involved in any required response, an explicit recognition of this authority by the governing board was deemed necessary and appropriate. A resolution, drafted jointly by the VPIT/CIO and university general counsel, was presented to the Board of Trustees' Finance and Audit Committee. However, after brief deliberation the board members chose to make the language stronger; indeed the final resolution *directed* . . . “the Office of the Vice President for Information Technology and CIO to develop and implement policies necessary to minimize the possibility of unauthorized access to Indiana University's information technology infrastructure regardless of the Indiana University office involved; and . . . draw[ing] upon the experience and expertise and resources of other University offices (including the Office of Internal Audit), to assume leadership, responsibility, and control of responses to unauthorized access to Indiana University's information technology infrastructure, unauthorized disclosure of electronic information and computer security breaches regardless of the Indiana University office involved” (Indiana University, 2001). The entire text of the resolution can be viewed at www.itpo.iu.edu/Resolution.html.

Closely following the adoption of this resolution, another well-publicized incident occurred involving the Indiana University School of Music in June 2001. Although it is difficult to quantify the effect that the resolution and the more active involvement of

the central IT security office may have had on the overall response to that incident, it is clear that the response was much smoother and much quicker. As one measure, notification of the potentially affected individuals, which included some individuals external to the university, took only seven days. In any case, after the two incidents and passage of the resolution, consultations with the central IT policy and security officers by department managers and technicians on security vulnerabilities, threats, and similar issues increased dramatically and are now commonplace.

This formal conferring of authority is analogous to the formal charge conferred on internal audit departments, which are generally separated from functions and operations and are at least partly responsible to the governing body of the institution. The resolution and the authority conveyed to the IU IT policy and security offices has smoothed significantly the path to an overall emphasis and improvement in IT security at Indiana University.

Conclusion

The need to improve computer and network security will make the combined strategies of security plans and policies an essential element of institutional processes that manage data or rely on computer networks. Planning for the protection of information resources and computer assets is no longer just the responsibility of the IT organization. The organizational value of networked information combined with the inherent risks in computer networks make IT risk management an increasingly important institutional priority. The development and enforcement of organizational policies requires engagement and support of the executive leadership as well.

References

- Association of College and University Policy Administrators. "Policy Development Process with Best Practices." [www.umd.edu/acupa/projects/process]. Apr. 2001.
- Barman, S. *Writing Information Security Policies*. Boston: New Riders, 2002.

- Desman, M. B. *Building an Information Security Awareness Program*. Boca Raton, Fla.: Auerbach Publications, 2002.
- Farnsworth, W. "What Do I Put in a Security Policy?" [www.sans.org/rr/policy/policy.php]. Apr. 2000.
- Indiana University. "Resolution of the Trustees of Indiana University Regarding the Leadership, Responsibility, and Security of IU's Information Technology Infrastructure." [www.itpo.iu.edu/Resolution.html]. May 2001.
- "IT Security Cookbook." [www.boran.com/security/IT1x-6.html]. July 2000.
- Joint Information Systems Committee. "Developing an Information Security Policy." [www.jisc.ac.uk/index.cfm?name=jcas_papers_security]. Feb. 2001.
- King, C. M., and others. *Security Architecture: Design, Deployment and Operations*. New York: Osborne/McGraw-Hill, 2001.
- Mandia, K., and Prorise, C. *Incident Response: Investigating Computer Crime*. New York: Osborne/McGraw-Hill. 2001.
- Nichols, R. K., Ryan, D. J., and Ryan, J.J.C.H. *Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves*. Washington, D.C.: McGraw-Hill, 2000.
- Peltier, T. R. *Information Security Risk Analysis*. Boca Raton, Fla.: Auerbach Publications, 2001.
- Peltier, T. R. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Boca Raton, Fla.: Auerbach Publications, 2002.
- Tudor, J. K. *Information Security Architecture: An Integrated Approach to Security in the Organization*. Boca Raton, Fla.: Auerbach Publications, 2001.
- U.S. Department of Education. "Safeguarding Your Technology: Practical Guidelines for Electronic Information Security." Washington D.C.: National Center for Education Statistics. [nces.ed.gov/pubs98/98297.pdf]. Sept. 1998.
- Walker, K. M., and Cavanaugh, L. Croswhite. *Computer Security Policies and Sun-Screen Firewalls*. Palo Alto, Calif.: Sun Microsystems Press, 1998.
- Wood, C. C. *Information Security Policies Made Easy*. (9th ed.) Houston, Tex.: PentaSafe Security Technologies, Inc., 2002.