

## CHAPTER 2 INSTRUCTIONS

---

This section provides an orientation to the information security policy writing process. While it might be tempting to immediately start cutting and pasting policies together, it is very important that these instructions are read (or at least scanned) before policy writing work gets underway. These instructions will provide background material that will make all subsequent policy writing tasks more efficient and focused.

This section provides guidance on the complex information security policy development process. This process includes writing policies, editing policies, obtaining management approval, communicating policies, and implementing controls to meet policy requirements. The last few subsections within this section contain hints and suggestions on how to best use this guide and the accompanying computer-readable material.

---

### INFORMATION SECURITY POLICIES

---

#### Distinct From Guidelines And Standards

Policies are management instructions indicating a predetermined course of action, or a way to handle a problem or situation. Policies are high-level statements that provide guidance to workers who must make present and future decisions. Policies are generalized requirements that must be written down and communicated to certain groups of people inside, and in some cases outside, the organization. Policies also can be considered to be business rules. Although information security policy documents vary from organization to organization, a typical policy document includes a statement of purpose, description of the people affected, history of revisions, a few definitions of special terms, and specific policy instructions from management.

Policies are mandatory and can be thought of as the equivalent of organization-specific law. Special approval is required when a worker wishes to take a course of action that is not in compliance with policy. Because compliance is required, policies use definitive words like “must not” or “you must.” The words used to compose policies must convey both certainty and unquestionable management support. For simplicity and consistency, throughout this guide, the word “must” has been employed, but equivalent words are acceptable.

Policies are distinct from, but similar to guidelines, which are optional and recommended. The policies appearing in this guide can be transformed into guidelines by replacing the word “must” with the word “should.” As easy as this substitution may be, the transformation of the policies found in this guide into guidelines is not recommended. This is because guidelines violate a basic principle of secure systems design called “universal application” which means

controls are significantly weakened if they are not consistently applied. Guidelines are desirable in some cases. For example, when work is to be done by a distributed group of individuals who cannot be compelled to comply with a policy, then a centralized information security function may appropriately issue guidelines as opposed to policies. This approach is commonly found when a centralized information security group issues a guideline for the preparation of departmental contingency plans.

Policies are higher-level requirement statements than standards, although both types of management instructions require compliance. Policies provide general instructions, while standards provide specific technical requirements. Standards cover details such as implementation steps, systems design concepts, software interface specifications, software algorithms, and other specifics. The term “information security architecture” is different then again, referring to a collection of integrated information security standards implemented across an organization, across operating systems platforms, and across networks. Standards would, for example, define the number of secret key bits that are required in an encryption algorithm. Policies, on the other hand, would simply define the need to use an approved encryption process when sensitive information is sent over public networks such as the Internet. An architecture would define a consistent approach to the implementation of various encryption processes across an organization, for example digital signatures and digital certificates.

Policies are intended to last for up to five years, while standards are intended to last only a few years. Standards will need to be changed considerably more often than policies because the manual procedures, organizational

structures, business processes, and information systems technologies mentioned in standards change so rapidly. For example, a network security standard might specify that all new or substantially modified systems must be in compliance with International Standards Organization (ISO) standard X.509, which involves authentication of a secure communications channel through public key cryptography. This standard is likely to be revised, expanded, or replaced in the next few years.

Policies are generally aimed at a wider audience than standards. For example, a policy requiring the use of computer virus software packages would apply to all personal computer users, but a standard requiring the use of public key digital certificates could be directed only at staff that conducts organizational business over the Internet.

## Distinct From Procedures And Controls

Policies are distinct from and considerably higher-level than procedures. These are sometimes called standard operating procedures or department operating procedures. A policy statement describes only the general means for addressing a specific problem. Procedures are specific operational steps or manual methods that workers must employ to achieve a certain goal. For example, in many information technology departments there are specific procedures for performing backups of server hard drives. In this example, a policy could describe the need for backups, for storage off-site, and for safeguarding the backup media. A standard could define the software to be used to perform backups and how to configure this software. A procedure could describe how to use the backup software, the timing for making backups, and other ways that humans interact with the backup system.

The need to clearly differentiate between policies, standards, and procedures is emphasized by International Standards Organization (ISO) 9000 Quality Standards for the preparation of internal documentation. For example, these ISO standards explicitly state that policies must be separate and distinct from procedures. In some organizations, policies become

detailed and lengthy, and in the process of development they become a confused combination of policies and procedures. While a clear demarcation between these document types is useful and highly recommended, nothing in this discussion is meant to imply that these different document types could not coexist in a paper binder or linked within an intranet documentation site.

Even more troublesome is the combination of policies, standards, and procedures in a single document. When it comes time to update such a document, the process is needlessly time consuming and confusing. This is because the three different document types all have different levels of detail and focus on different things. Because these three document types are intended for different audiences, this combination approach also runs a high risk that the material will not be read. People are very pressed for time, and if a document contains a lot of material that is not relevant to them, they will be likely to stop reading. The combination of policies, standards, and procedures in a single document is also not recommended because it can make the location of relevant information much more difficult for the reader. This combination approach is inefficient in terms of distribution because a lot of irrelevant information is sent to people who do not need it. To simplify document maintenance, usage, and cross-referencing, be sure to use separate documents for policies, standards, and procedures.

Policies are different from controls, also known as countermeasures, security measures, and safeguards. A control is a device or mechanism used to regulate or guide the operation of a machine, apparatus, system, or process. An example of a control would be encryption of sensitive data stored on floppy disks. In many cases, policies provide broad objectives that are met with controls. For example, a policy prohibiting actual or apparent conflicts of interest could be partially met through a control requiring employees to sign a statement indicating they have read the code of conduct and agree to comply. Likewise, in many instances, control measures are dictated directly by policy. For example, a requirement to sign a statement of compliance with a code of conduct might itself be a policy.

## IMPORTANCE OF POLICIES

---

With all of the attention that information security receives from the news media, one may believe that management understands what an information security policy is and why an information security policy is necessary. Unfortunately, this is often not the case. Before writing a policy document, management should be consulted to ensure that they are all talking about the same thing, and that they understand why a policy development effort is important.

The prior subsection, “[Information Security Policies](#),” provides specific words that can go into a memo to clarify work results. The sample policies at the end of this guide also can be submitted to management as rough approximations of the finished products that will be produced. The following section provides specific ideas that can go into a memo detailing the reasons why an information security policy is important. A summary of justifications for the adoption of information security policies is provided in the table labeled Table 1. Some of the more important reasons to have information security policies are described in their own subsections immediately following the next subsection.

### Assuring The Proper Implementation Of Controls

With hopes of handling information security expediently, management in many organizations simply purchases one or more information security products. In these cases, management often thinks the new products, such as hardware, software, information content, or services, are all that is needed. Soon after the products are installed, management is often disappointed to learn that the anticipated results have not materialized. In a large number of instances, this disappointment can be traced to the fact that management has failed to establish an adequate organizational infrastructure for information security. And one of the most critical components of an organizational infrastructure for information security is a policy document.

An example should clarify this essential point. Suppose that a large organization has recently acquired a single-sign-on access control package for a multi-user computer system such as a super-server attached to an intranet. Simple installation of the package will do little to improve security. Management must decide which users should be given access to which information resources, preferably defining the ways to make these decisions in a policy. Management must establish

procedures so that the technical staff can configure access controls in a manner consistent with these decisions. Management should assign responsibilities for reviewing system logs and other records generated by the access control package. These and other efforts constitute part of the necessary organizational infrastructure to support security products. Unfortunately, most information systems technology vendors do not provide policies, procedures, roles and responsibilities, and the other parts of an organizational infrastructure necessary for the immediate usage of their products. The organization purchasing these products must instead come up with an organizational infrastructure. In part this is because organizational infrastructure is a function of, and must respond to, each organization's unique requirements.

To establish a supporting organizational infrastructure, every organization needs a variety of documents. These include organizational responsibility statements, policies, standards, operational procedures, and enforcement mechanisms. Several management processes also are needed. These include a risk assessment process, a process for coordinating an information security management oversight committee, and an information security budgeting and planning process. Once responsibility for information security has been defined in departmental mission statements and job descriptions, the next step is to perform a risk assessment. Once an initial risk assessment is completed, an initial information security policies document should be prepared. Other documentation such as standards and operational procedures then grow directly from the policy document and subsequent efforts. The timing issues surrounding the preparation of policies are discussed in greater detail below in the subsection entitled “[Policy Development Time Line](#).”

### Guiding The Product Selection And Development Process

Most organizations do not have the resources to design and implement their own controls. They often pick and choose from the set of controls provided by information security product vendors, and they attempt to customize these controls with policies, procedures, standards, and other organization-specific integration efforts. This custom integration process is often performed without sufficient understanding of the security objectives and goals of the organization. As a result, the security products chosen and their implementation may not be

responsive to the true needs of the organization. For example, the purchase of devices to bolt computers to desks may have been motivated by a number of thefts. In the absence of guiding policies, management may have selected a product that does not easily permit the secure storage of portable computers.

To avoid these problems, policies stating information security objectives and requirements can provide both the understanding and additional guidance that workers need in order to act as management intends they should. Such policies can be a way to ensure that in-house personnel are appropriately selecting, developing, and implementing information systems. For example, a policy can state that only virus screening software approved by Information Security Department may be used on Company X systems. The actual vendor and product name can change from month to month without the need to change the policy. These details could instead be found in a standard.

## Demonstrating Management Support

Some people, particularly users and Information Technology Department staff, often say, “When management tells me to, then I’ll do something about information security.” This attitude is not surprising when one appreciates that most people are unaware of the extent of the information security risks they face, just as they are not inclined to take the time to seriously analyze these risks. Beyond this, because they do not have the expertise, most people are unable to evaluate the need for certain control measures.

Policies are a clear and definitive way for management to demonstrate that information security is important, and workers must pay attention to information security. Policies can compensate for influences that may otherwise cause people to insufficiently protect information resources. One frequently-encountered example involves middle-level managers who repeatedly refuse to allocate money for information security in their budgets. In this case, the other influence is often a bonus plan that rewards them for keeping costs down. But if policies dictating management support have been issued by top management, then middle-level managers will have difficulty if they continue to deny requests for information security funding.

## Avoiding Liability

In addition to explicit statutes, an increasingly compelling body of case law is demonstrating that management and even technical staff may be held liable for

inadequately addressing information security matters. The basis for this liability can be negligence, breach of fiduciary duty, failing to use the security measures found in other organizations in the same industry, failing to exercise the due care expected from a computer professional, or failure to act after an actual notice or compromise has occurred. Discussions about liability exposure and the need for policies are often successfully used to gain additional management attention and support for information security efforts. Internal legal counsel should be consulted prior to covering this topic with management.

Policies have been shown to be influential evidence in the eyes of the court that management has been concerned about and done something about information security. If the organization has not yet seriously addressed information security, it is important to promptly start work and to set the direction for future efforts. From a legal standpoint, the first line of defense is evidence that you are doing something about it, and you have documentary evidence to prove these efforts.

## Demonstrating Compliance with Regulations

Many organizations are now getting senior management support for information security due to regulatory requirements. Within the last several years, federal or state regulations involving the security and privacy of information have impacted nearly every industry. The complexity of international data privacy laws has also added an extra policy burden to organizations that do business internationally. The possible risk of steep fines, personal liability of executives, bad publicity and/or de-listing from a stock exchange are generally enough to boost management's support for information security. Security and privacy regulations are very specific about the requirements for written security policies. See Appendix O, “[Regulatory Requirements for Information Security Policies](#)” for a list of various security and privacy-related regulations and their specific policy requirements.

## Protecting Trade Secrets

Although the laws related to trade secrets vary from jurisdiction to jurisdiction, policies can provide extra protection for sensitive intellectual property. In a court of law, policies can serve as evidence indicating that an organization seriously took steps to protect its sensitive intellectual property, convincing the court that such intellectual property should be deemed a trade secret. If information is deemed a trade secret, an organization

has additional legal remedies available that may make a case for larger monetary damages or the issuance of an injunction. [Table 2-1](#) includes a variety of reasons for establishing information security policies within your

organization. You may wish to use some of these ideas in a memo to management which suggests that policies be developed or revised.

Table 2-1: Reasons To Establish Policies

| Reason  | Result   |
|---|--|
| Expand information security budget and add more personnel.        | Policy development process shows management what is needed.  |
| Establish top management communication path.                      | Participation of management in the development process opens new channels.   |
| Show definitive progress with minor investment.                   | Only days or weeks are required to generate a credible policy document.  |
| Establish information security effort credibility and visibility. | A policy document should have a chief executive officer's signature on the cover page.   |
| Shift worker attitudes and change perspectives.                   | The support of all workers who interact with information systems is mandatory and now it's in writing.                                     |
| Harmonize and coordinate the activities of many workers.          | Consistent action is required if security is to be achieved and maintained.  |
| Define the boundaries of permissible action.                      | Workers will clearly understand how far they can go when they use information systems like the Internet.                                   |
| Control security-relevant events in advance.                      | Increases chances that things will be done correctly the first time, reduces errors, and allows rapid responses to attacks.                |
| Exercise control by exception rather than micro-management.       | Every action and decision is not going to be reviewed, and this reduces costs.   |
| Overcome ambiguity that can lead to information overload.         | A policy document will focus worker attention on the essentials of information security.   |
| Permit management to determine if a worker used poor judgment.    | No disciplinary action is called for if poor judgment was involved, but it is appropriate if a worker acted in opposition to instructions. |
| Avoid disputes and related internal politics.                     | Staff can focus on business problems instead of who is responsible for information security and what should be done to handle security.    |
| Enable rapid development of new systems.                          | Many of the requirements will have been defined in advance so that they need not be revisited.   |

Table 2-1: Reasons To Establish Policies (Continued)

| Reason  | Result  |
|---|---|
| Coordinate activities of internal and external groups.              | Policies will enable an extranet to be established or outsourcing organization to be used.  |
| Achieve lower costs through control standardization.                | The same approach can be used consistently throughout the organization, and volume purchase agreements can be negotiated.                   |
| Avoid problems because tasks are out of sequence.                   | On critical issues, staff will not be required to guess how to proceed.   |
| Prevent all decentralized groups from "reinventing the wheel".      | By specifying policies centrally, local groups need not develop them.   |
| Establish a starting point for a process of continuous improvement. | Policies are a baseline that can be referred to and improved upon.  |
| Demonstrate quality control processes.                              | ISO 9000 compliance requires that business rules be clearly documented.   |
| Establish benchmarks or reference points for future audits.         | Internal auditors can determine whether compliance exists.  |
| Guide security product, and service selection and implementation.   | Uncoordinated local groups are less likely to go their own way.   |
| Assure consistent implementation of controls.                       | Each exception weakens a control, and policies can mandate control compliance across the organization.                                      |
| Demonstrate compliance with laws and regulations                    | Written policies provide evidence of management support and document security program requirements.   |
| Arrange contractual obligations needed for prosecution.             | Use policy compliance agreements and confidentiality agreements, non-compete agreements, and related documents to create legal obligations. |

## Adapting To A Dynamic Communications Environment

Workers in modern organizations are increasingly showing signs of burnout and information overload. The proliferation of new communications technologies such as computers, the Internet, fax machines, photocopying machines, and pagers has destabilized long-standing communications processes. For example, while it used to be polite behavior to return all telephone

calls, this is no longer standard procedure if the one requesting a callback is known to be a salesperson. The lack of clear rules dictating appropriate behavior in this dynamic environment has made life more difficult for workers. To effectively manage worker expectations and to effectively guide behaviors, management must dispel this ambiguity by setting clear priorities and defining appropriate actions. The policy messages contained in this book and CD-ROM are intended to do just that for the information security domain.

## Achieving Consistent And Complete Security

One of the most serious problems in the information security field involves fragmented and inconsistent efforts. Too often one department will be supportive of information security efforts, while another department within the same organization will be resistant. To the extent that these departments share computing resources, such as an intranet, the resistant department will be likely to jeopardize information security in the supportive department. This could, for example, take place if a hacker were to gain access to an intranet through lax dial-up user authentication processes within a resistant department, and then leverage this penetration to gain additional access that the hacker would not otherwise have been able to obtain. Although it is neither feasible nor desirable to make all persons in an organization familiar with the complexities of information security, it is important that they all subscribe to some minimum level of protection. In high-level terms, policies can be used to define this minimum protection level, sometimes called a baseline.

## Coordinating Activities Of Internal And External Groups

Outsourcing and the use of contractors, consultants, and temporary personnel have become business necessities at many organizations. Likewise, today's organizations are also establishing close business partnerships with a variety of organizations, and in some cases these organizations are competitors. The large number of participants in business has made system access control,

intellectual property protection, and related information security issues more difficult to manage. Because so many different parties are involved, there is a pressing need to consistently coordinate the activities of both internal and external groups. That is where information security policies can help. For example, a policy can address the circumstances where a confidentiality or non-disclosure agreement is necessary, and where it is not. Managers hiring contractors can then read this policy and manage these contractors so that internal information assets are properly protected.

In days gone past, sensitive information was often concentrated in the hands of middle and top management. These days, information is being pushed down the organizational hierarchy, out to lower-level employee desktops, and even further out to contractors, consultants, and temporaries. As a larger number of individuals get involved in the information management area, and as a larger number of people gain access to sensitive, valuable, or critical information, there is an increase in the need for information security policies.

Direct supervision of all of these people is impractical, and cost-effective technological tools to monitor every action they take are not yet available. Although organizations will rarely admit it, all of these people need to be self-managed, but they need instructions in the form of information security policies in order to do it right. The state-of-the-art in information security involves significant unsupervised reliance on people because sophisticated tools are not yet available. The number one tool for managing the behavior of people in the information security area is a policy document.

## CONSIDERATIONS IN THE POLICY DEVELOPMENT PROCESS

---

### Gathering Key Reference Materials

Information security policies should be largely driven by the nature of the information handled by the organization. A government agency that handles tax collection will be focused on privacy policies, while a retail bank that does a lot of Internet payment processing will be focused on fraud. Before writing any policies, the policy writer should take the time to acquaint him- or herself with the nature of the information handled by the organization. A good source for this information, also known as metadata, is a data dictionary. Overviews of internal information systems prepared for top executives, board members, merger and acquisition candidates, and strategic partners, also may be useful

background to the policy writing effort. Because information systems change so rapidly, available documentation is likely to be outdated. Knowledgeable workers should be interviewed to accurately identify the nature of the information currently being handled by the organization, including what information is sensitive, what information is valuable, and what information is critical.

When developing a set of information security policies, a recent risk assessment or an information technology audit should be referenced that clearly indicates the organization's current information security needs. A loss history documenting the specifics of recent incidents, may be helpful in terms of identifying areas in need of further attention. Lawsuits, formal written grievances,

and other disputes may identify areas that should be addressed in a policy document. To identify further problem areas, meetings with interested parties such as the Chief Legal Counsel, the Physical Security Manager, the Chief Information Officer, the Internal Audit Manager, and the Human Resources Manager are advised.

To identify the policy areas needing further attention, copies of all other relevant and current organizational policy documents should be collected. Relevant policies include application systems development policies, computer operations policies, computer equipment acquisition policies, human resources policies, information system quality control policies, and physical security policies. If they are obtainable, policies from other organizations in the same industry can provide useful background information. If the organization is a subsidiary or affiliate of another organization, then the parent organization's policies should be obtained and used as reference material. If the organization is a participant in an extranet, an electronic data interchange, value added network, a multi-organizational Internet commerce arrangement, or any other multi-organizational networks, the policies of these networks should be obtained and reviewed. The security policies of various information systems related service providers, such as an Internet service provider, should also be obtained.

Some policy writers who are facing significant time or resource constraints will be tempted to skip the above-mentioned data gathering processes. Whenever data gathering is significantly abbreviated, the likelihood that management will reject the resulting document increases dramatically. It is through this data gathering process that management's view of information security, the policies that already exist, the policies that need to be added or changed, how management enforces policies, the unique vulnerabilities that the organization faces, and other essential background information, will come to light. If serious consideration has not been given to this background information, it is unlikely that a newly written information security policy will be responsive to the true needs of the organization.

Another major reason to do a good deal of background research in preparation for policy writing is to ensure that the requirements defined in the policy document are consistent with management's intentions. One of the fastest ways to lose credibility for an information security policy writing effort is to propose a policy that is clearly inconsistent with existing organizational norms. For example, employees at high-tech company routinely downloaded games from the Internet and played these games on their powerful workstations during breaks and

after-hours. Top management knew of and tacitly approved of these activities. At the same time, a published policy indicated that no personal use of the corporation's information systems would be tolerated. This glaring inconsistency caused a large majority of the workers at this company to dismiss the policy document as irrelevant.

Another important reason to spend considerable time on background research is to identify and define the organization's business-related strategic directions. A new or revised policy document needs to be consistent with these strategic directions if top management is going to approve and support the policy. For example, suppose an organization decides it wants to once again centralize its currently decentralized information systems activities. A policy document that stresses many activities to be performed by a group of decentralized information security coordinators would then be inconsistent with management's intentions, and consequently would be unlikely to be approved.

Yet another reason to thoroughly research the current situation before beginning the policy writing process is to identify the internal information systems architecture. An information security policy document should be consistent with and fully support an existing information systems architecture. Note that we are NOT talking about an information security architecture here, but an information systems architecture. An information security policy document is typically developed after an information systems architecture is already in place. The development of an information security policy document will then permit an information security architecture to be developed. For example, a policy about permissible access through an Internet firewall will enable a security architecture to be specified. Such a policy will also enable an appropriate firewall product to be chosen and implemented.

## Defining A Framework For Policies

After the above-mentioned reference materials have been collected, a list should be compiled that contains topics to be covered in a new or revised information security policy document. The first draft of the list should include policies that are intended for immediate adoption and those that are intended for adoption in the future. In most cases, the level of detail in this list will be inconsistent, and at this stage in the process, this should not be cause for concern. For example, the list might include telecommuting and password construction with a minimum of 10 characters. When a high level outline

is prepared, the level of detail should be standardized. For more information about this, see the section below entitled “[Preparing A Coverage Matrix](#).”

Next, an attempt should be made to define the ways in which the organization intends to express information security policies. For example, policies may be placed in a standard operating procedures manual. Alternatively, the director of the Information Security Department may periodically issue electronic mail memos summarizing policies. It is common for privacy policies to be posted on Internet web pages. Because workers are bombarded by communications from many people through many different communication channels, it is essential that information security policies be repeated sent through multiple communication channels. For more information about suggested ways to communicate policies, see Appendix D, “[List Of Suggested Awareness-Raising Methods](#).” The channels used to express a policy will determine how the policy should be written. For example, if videotape will be used, then an abbreviated colloquial style should be employed. If a policy document will reside on an intranet web server, then a more graphic and hypertext-linked style is appropriate. If policies will be issued through a series of paper memos, then short and concise text-oriented expressions will be required.

The ways that the organization currently uses or intends to use information security policies should also be examined. Policies may be used to guide information system acquisition efforts, drive information technology audit plans, and assist users in securely operating their desktop computers. For additional ideas about potential uses, see [Table 2-1](#) entitled “[Reasons To Establish Policies](#).” Defining the uses of policies will identify the audiences to whom policies will be addressed. For more information about identifying audiences, see the subsection below entitled “[Preparing A Coverage Matrix](#).”

Determining the uses for policies will also help focus attention on those areas that most need to be addressed. Other uses soon will be apparent after the policy document has been distributed. This should not be considered poor planning, but should be considered a successful initiative that has unforeseen contributions to the organization. In some instances, the uses of a policy document will be initially unknown, but these uses can be quickly identified through a series of meetings with interested parties.

The policy writer should study the style in which existing policies are written, the use of certain words, the conventional format for documenting policies, the system for numbering and naming policies, as well as the

linkages between policies and other management directives like procedures and standards. For example, existing policies may use the word “must” consistently. To maintain consistency, the new information security policies also should use the word “must.” Likewise, the existing policies may have a military-style numbering system, in which case new information security policies should also use this same system. The issuance of an information security policy document will be controversial by nature. The policy writer should not give critics additional ammunition by failing to be consistent with internal policy style guidelines, whether these guidelines are written or unwritten.

Part of the study of the existing policies and how they are used should entail a review of the level of detail appropriate for the organization’s policy statements. The organization may have defined existing policies in very specific terms, in which case many detailed information security policies may be appropriate. Alternatively, the organization may have defined policies in very high-level terms, in which case only a brief overall information security statement may be appropriate. Both of these alternatives may simultaneously exist in that separate policies are provided to different audiences. The level of detail is in part driven by the extent to which management trusts workers to use their own judgment, the extent to which ISO 9000 and other specific documentation requirements are being observed, and the extent to which the topics being addressed are new to the involved audiences.

Information about the expression, use, style, and level of detail found in internal policies is rarely documented, but it can be obtained by examining existing policy statements. In very large organizations there may even be a document that provides directions on the policy writing process. In some large organizations, in-house staff in a Policy & Planning Department can help with a policy writing effort. Whether or not explicit written guidance or in-house consulting assistance are available, to ensure their prompt adoption, new and revised information security policies should be written in a manner that resembles and is at least in form indistinguishable from existing policies.

## Preparing A Coverage Matrix

After preparing a rough list of the areas needing attention, and after becoming acquainted with the ways in which the organization expresses and uses policies, the policies found in this book and CD-ROM can then be used. At this point the policy writer is looking for topics to be covered in the new policy document. The

policy writer should review the Chapter 3 subsection titles, the policy titles, and in many cases the policy text statements, but skip the accompanying policy commentaries. This task is generally done most rapidly with the hardcopy guide and a marker such as a yellow highlighter.

To obtain additional ideas for the areas to be covered, this guide's Table Of Contents can be used. While the Table of Contents is useful and does provide good coverage of the major topics, categories should be developed that uniquely respond to the organization's needs. Alternatively, categories reflecting the areas to be addressed also may be patterned after an internal audit report or an information security guide that management values. Another way to segment the controls would be broad control objectives such as "avoid," "prevent," "deter," "detect," "mitigate," "recover," and "correct." Yet another way to organize a policy document would be along technological lines, such as telecommuting, desktop computing, intranet, Internet, extranet, etc.

At this point, a draft high-level outline reflecting the topics to be addressed should be developed. This outline is best if accompanied by a brief explanation with examples of topics to be covered in each section. The explanation can be only a sentence or two and just enough to provide a preview the topics included. At this point, distribution of the high-level outline to interested parties is recommended, and the constructive feedback received should then be integrated with the high-level outline.

At this point, a determination must be made of the proper audiences to which these messages are to be addressed. Often policies will be directed at several significantly different audiences because each audience has distinctly different needs. For example, end users might receive a small booklet containing the most important information security policies that they need to keep in mind. The focus could be on desktop computer information security issues. At the same time, systems developers and other technical staff might receive a considerably longer document that provides much more detail, perhaps focusing on security as part of a standard systems development methodology. Management may get yet another document that deals primarily with the tasks of information Owners.

While separate documents for separate audiences may sound like too much effort, the additional work is not great if a list of the essential messages to be communicated has been made in advance. This list can be split by audience, and it is this splitting process that is discussed in the next few paragraphs. The development and

maintenance of separate documents for separate audiences is much easier if all of these documents are placed on an intranet. Using browser links, those who read the policy can be quickly provided with only the information that is relevant to them. For example, at a large bank, an intranet is used to segment the information security policies by job title. People need to read only those policies that directly apply to their own job. This intranet implementation also provides a key word search mechanism and an index, both of which help readers quickly find policies relevant to their current circumstances. Intranets can also now be used to administer quizzes to ensure that policies were understood.

When more than two audiences will be addressed by separate policy documents, it is recommended that a "coverage matrix" be prepared before actually writing the first draft policy documents. This can be achieved by preparing a separate detailed outline for each of the identified audiences. A coverage matrix is simply an organizational tool to ensure that all the appropriate information security policy messages are presented to all the appropriate audiences. It is a way of looking at the work to be done and can bring order to what otherwise may be a complicated policy writing effort. Once the topics to be communicated have been identified, and organized in a coverage matrix, the preparation of policy documents will be relatively easy and straightforward.

A coverage matrix in its simplest form is a two-dimensional table. It can, for instance, use the primary audiences to which the policies are directed as row identifiers, and policy categories as column headings. These policy categories are the major sections appearing in the above-mentioned high-level outline. The cells in the center of the matrix should be filled with reference numbers, each referring to a policy found in this guide and perhaps elsewhere.

Because there will probably be many columns, but only a few rows, a standard coverage matrix with the row identifiers filled in for audiences, with blank column identifiers for policy categories, and with blank cells in the middle for specific policies is recommended. Such a template coverage matrix then can be photocopied many times to save considerable time creating coverage matrices. If seeing only one portion of the coverage matrix at any one moment is acceptable, it is often more time-efficient if a spreadsheet program is used to construct and manipulate a coverage matrix. Use of a spreadsheet program also makes the generation of professional-looking hardcopy easier, just as it makes updates more straightforward. Another reason to use a spreadsheet for the preparation of a coverage matrix is

the fact that it can be searched using key words, in this case a key word would be a specific policy number, or a specific policy category which would be only part of a full policy number as shown below in [Table 2-2](#).

Often only two or three audiences will be needed. Two possible audiences could be end users and computer-literate technical staff. Using another approach, three possible audiences could be end users, management, and computer support. In almost every instance, there will be a significant amount of overlap in the messages directed to each of these audiences. The policy writer should make every attempt to minimize the number of audiences at the same time recognizing the real needs of different groups to receive different information.

[Table 2-2](#) provides an example of a coverage matrix that a policy writer might develop. The policy numbers appearing in this matrix are place holders and are deliberately not the result of an analysis. This was to discourage the policy writer from simply using these numbers rather than performing his or her own analysis.

Each organization will need to prepare its own coverage matrix, inserting policy numbers in the relevant cells to reflect its own unique business and information systems environment.

If the development of this type of a coverage matrix seems too time consuming, a similar table using broad categories such as those found in the Table Of Contents to this guide can be prepared.

An alternative approach provides what could be considered a middle ground between a single policy and separate policies for different audiences. In this case, a broad umbrella policy document can apply to all staff, while separate specialized policy documents can be used to address audiences such as information owners, systems developers, telecommuters, and other target audiences. With this approach there is a basic set of rules that applies to everyone, but then there are also special policies that apply only to selected audiences. At larger organizations with intranets, this approach is increasingly common.

Table 2-2: Sample Coverage Matrix

| Audience                       | Computers  | Data Communication   | Risk Management  | Physical Security  |
|--------------------------------|--|--|--|--|
| End Users                      | 9.03.01.08<br>9.03.01.09<br>9.05.04.13<br>9.06.01.02                 | 9.02.03.11<br>9.03.01.09<br>9.03.01.10<br>9.03.01.11<br>9.03.01.12<br>9.04.03.03<br>9.05.04.13<br>9.06.01.02 | 5.02.01.02<br>5.02.01.03<br>8.07.06.31   | 9.05.04.13<br>9.05.04.22<br>9.06.01.02<br>10.03.02.11  |
| Management                     | 9.04.07.01<br>9.05.04.13<br>9.05.04.22<br>12.01.03.02<br>12.01.04.23 | 12.01.04.04<br>12.01.04.87<br>12.01.04.88<br>12.01.04.89<br>12.01.05.16<br>12.01.07.03                       | 9.03.01.08<br>9.03.01.10<br>9.03.01.11<br>9.03.01.12<br>9.02.03.09<br>9.02.03.10<br>9.02.03.12<br>9.04.03.04 | 8.04.01.15<br>8.07.05.47<br>8.07.05.48<br>9.03.01.07<br>9.03.01.08<br>9.04.07.01<br>9.05.04.22<br>9.05.05.06<br>9.05.05.07<br>9.05.06.01<br>9.06.01.02<br>10.04.02.02<br>12.02.02.01     |
| Information Systems Department | 9.04.03.04<br>9.05.03.03<br>9.05.04.22                               | 8.03.01.15<br>10.02.02.02<br>10.02.02.03   | 6.03.01.04<br>8.06.01.01<br>8.06.03.06   | 8.01.02.01<br>8.03.01.19<br>9.02.01.01<br>9.05.04.08<br>9.05.04.13<br>9.05.04.17<br>9.07.02.16<br>10.02.02.05<br>10.05.01.07<br>10.05.01.08<br>10.05.01.09<br>10.05.01.10<br>12.01.04.20 |
| Customers                      | 8.03.01.20<br>8.03.01.21<br>10.05.01.14                              | 10.01.01.06<br>10.01.01.07<br>10.05.01.04  | 9.05.03.03<br>9.05.04.22<br>9.05.04.23<br>9.05.06.01   | 9.05.03.03<br>9.05.04.23<br>9.05.06.01<br>9.06.01.02   |
| Business Partners              | 8.02.02.07<br>8.02.02.08<br>8.02.02.09                               | 5.02.02.04<br>10.01.01.08<br>10.01.01.09   | 9.03.01.04<br>9.03.01.05<br>9.03.01.06<br>9.05.04.24   | 8.07.06.09<br>9.05.02.01<br>12.01.04.32<br>12.01.04.42<br>12.03.01.01  |

In an effort to save time, some people often anticipate there will be only one audience. This one-size-fits-all approach may work for the first few policy statements that an organization issues, but the more sophisticated the information security effort, the less applicable this

approach will become. It will often save a significant amount of time if the different audiences are targeted from the beginning of a policy writing effort, rather than having to keep modifying a one-size-fits-all policy that was originally intended to meet the needs of multiple

audiences. The various audiences will also appreciate the use of separate documents. If separate documents are employed, they will not need to be repeatedly notified about changes that in many cases will not apply to them. The use of separate documents will permit differential treatment without confusion. For example, the rules for third-party access to an organization's information systems can be quite different from the rules for permanent full-time employee access.

Just because there are different audiences for policies does not necessarily imply that there should be different documents. It is possible to have different chapters or sections in an information security manual devoted to different audiences. This approach is attractive because all the policies are then found in one document rather than several. Having all information security policies in a single manual facilitates maintenance and revisions. It is also attractive because individuals often find themselves falling into two or more of the audiences. For example, an individual may be both a general user and a systems developer.

At this point the policy numbers should be written directly into the body of the coverage matrix. The process of filling in the body of the coverage matrix often highlights the fact that certain audiences are not being adequately addressed, just as it often indicates that certain areas need additional policies to be truly responsive to the organization's needs. If outlines for policy documents to different audiences were prepared, but no coverage matrix was used, these discrepancies may not have been revealed.

If an area is not adequately addressed, this guide's indexes or Table of Contents can be referenced to obtain additional ideas. The CD-ROM provided with this guide can be searched based on key words. For example, if additional virus policies were needed, a search for the word "virus" would quickly yield results.

After the overall topics to be covered have been clarified through a coverage matrix, a detailed outline of the soon-to-be-prepared policy documents can be compiled. Depending on the management at the organization, there may be a need to get interested parties to review a detailed outline. If no such review is required, then a detailed outline may not be needed. In this case, using the coverage matrix, the first draft policy documents can begin to be prepared.

Those policy writers who have noticed a great deal of political uncertainty associated with the policy writing process within their organization may wish to prepare a detailed outline and then put it through a review

process. While this may delay the process, it ensures that the resulting document is on target and truly responsive to the organization's needs. Where only one audience is being addressed, the coverage matrix can be dispensed with, but a detailed outline is still needed. Either a coverage matrix or a detailed outline is important. Without one or the other, the policy writer risks weeks of wasted time writing policies on topics that are not needed or not wanted by management.

At this point, a decision on the categories to be employed in the policy document must be made. The categories in the coverage matrix or the detailed outline will do, although they will often be modified during the subsequent review process. As an aside, the use of a large number of subtitles is recommended. This will assist readers in their efforts to quickly locate topics of interest. This will permit readers to skip sections that do not pertain to them.

In those cases where a very large policy document is being developed, or if a significant amount of complexity must be addressed in the policy document, a mind map can be used. Mind maps are graphical representations of the relationships between ideas. They generally use circles to represent ideas and arrows to represent the relationship between ideas. A mind map can be readily converted into a complex outline, which in turn can be used to develop a draft policy document. Various guides and software programs are available to assist with the drawing and revision of mind maps. One of the best books describing the mind mapping process is "Writing The Natural Way" by Gabriele Lusser Rico (published by J. P. Tarcher, Los Angeles, California, USA, 1983).

After the policy writing process is complete, the coverage matrix, outlines, and related working papers should be saved. In a year or two a revised policy document will probably be needed. It will save a lot of time if the person writing revised policies can consult the original working papers. The coverage matrix and related working papers may also serve as important information in a court case, should there ever be any allegations that management did not seriously think about the risks and the policy messages that needed to be communicated.

Similarly, the working papers should be retained for a year or two because internal and external auditors may wish to review them. Having the working papers in an accessible storage location can also be important if a member of the management team claims that his or her comments were not considered or not adequately integrated into the final draft policy document.

## Making Critical Systems Design Decisions

Before a final version of a policy document can be published, management often needs to make a number of security-related systems design decisions. Examples of these decisions include the:

- Groups of users that will be given Internet access.
- Frequency that these users will need access, whether continuous, regular, or occasional.
- Type of access they will need, whether electronic mail, web surfing, file transfer, remote logon, or chat rooms.
- Type of access they will need, including electronic mail, web surfing, file transfer, remote logon, and chat rooms.
- Type of access control, including dynamic passwords, fixed passwords, or smart cards.
- Types of user activity that will be monitored, including files transferred, web sites visited, and hours per day of usage.

Identification of these and other systems design decisions is ordinarily indirect. Typically a draft policy document that incorporates a number of suggested options will be prepared. Unfortunately, in an effort to expedite the policy writing process, alternative solutions are not highlighted. As a result, management may approve of a policy document incorporating decisions with far-reaching implications, many of which were unappreciated at the time of the approval. This may lead to excessive costs for information security as the initial approaches described in the policy document soon need to be replaced or revised. It may also mean that the policy document needs to be changed much sooner than it otherwise would be.

If the project schedule and resources permit, the fundamental systems design decisions should be highlighted. If a paper draft of the policy is going to be circulated for comment, this could be accomplished by using footnotes or endnotes that describe the options and the pros and cons of each. Wording reflecting the different design decisions can be incorporated into the body of draft document. Seeing the options in context will often help management make these decisions. If the draft policy is going to be placed on an intranet server with restricted access to selected interested parties, certain words can be highlighted and links can be used to illuminate options and supporting justifications.

In organizations that have been attending to information security for some time, management will have already seriously considered all the necessary fundamental systems design options. In these cases, a policy writing effort will simply involve documenting the decisions already made, and choosing appropriate ways to express these decisions in the form of policies. In these cases, there will be no need for a separate review of the critical systems design issues as discussed above. Instead, the focus can be on the extension of these existing design decisions to new information systems such as extranets, and to new technologies such as new programming languages.

## Structuring Review, Approval, And Enforcement Processes

Once the first draft of the information security policy document has been written, a few colleagues should review them. After the changes are made in response to feedback from these colleagues, the policy document should be sent to interested internal parties such as the Internal Audit Manager and the Intellectual Property Attorney. After a few critical allies have made changes, it is ready for review by the Information Security Management Committee. The next release of the draft can involve distribution to a much larger body of interested parties, for example all information Owners and all technical staff in the Information Systems Department. This review process is advisable because it builds on support from critical players, pre-selling the document to these critical players, and building support from these same critical players.

Many review cycles, each with more changes to the policy document, are often necessary. This should be viewed as standard procedure, and should in no way be taken as a personal insult. Multiple reviews are in part a reflection of the fact that the information security policy development process is highly political, emotionally-charged, and highly unstructured. Input should be welcomed with an appreciation that this iterative review process makes the policies more clear, concise, and responsive to prevailing conditions. Two appendices to this guide provide additional information on this process. For more information, see Appendix G, “[Overview Of Policy Development Process Tasks](#)” and Appendix E, “[Checklist Of Steps In Policy Development Process](#).”

The final step in the review process is the signature of the general manager, president, chief executive officer, or chairman of the board. A brief message indicating that compliance is expected as a condition of continued

employment should be found on the first page of a policy document, or the opening web page if the policy is posted on an intranet server. This message should be signed by the top executive in a readily visible place so that the reader can have no doubt that the policy document is strongly supported by top management. If there is no realistic chance of getting the chief executive involved, the signature of the Chief Information Officer may suffice. Settling for the approval of a middle-level manager is not recommended. The signature of the Information Security Manager is generally insufficient to show top management adoption and support. While obtaining top management approval may sound like unnecessary marketing, experience has shown that a top management signature and accompanying message about expected compliance is critical to widespread adoption. Before management approves a policy document, it should already have been reviewed and edited several times by various parties within the organization. Perhaps the most desirable review body is an Information Security Management Committee.

An Information Security Management Committee is generally composed of representatives from departments within the organization who are interested in information security. Participants include members from the Information Security, Internal Audit, Risk Management, Physical Security, Information Systems, Human Resources, Legal, Finance, and Accounting Departments, as well as various user departments. Such a committee typically oversees the work of the Information Security Department. This management committee is used to filter and refine proposed policies, procedures, organizational structures, and other information security initiatives so that they will be readily adopted and implemented throughout the organization. In most cases, a senior staff member in the Information Security Department will write a draft version of an information security policy, then submit it to the Committee for review and approval. If the organization does not yet have such a committee, development of an information security policy is an excellent time to propose the formation of such a committee. The Committee is generally made up of five to eight individuals who have relevant expertise, who are seen as influential in the information security area, and who can represent their own department or area of expertise. For more information about such a committee, see the author's book and CD-ROM entitled *Information Security Roles & Responsibilities Made Easy*. Within this book, the policy entitled, "[Information Security Management Committee](#)" also provides some guidance.

In some cases, a separate Information Security Policy Development Committee is formed. Such a committee could be formed regardless of the existence of an Information Security Management Committee. This development committee may be a subcommittee of the Management Committee. If a Development Committee is created, it should not actually write the policy. Policies written by committees are often a combination of inconsistent ideas, poorly-organized thoughts, and divergent ways of expressing concepts, that never seem to coherently come together into an integrated and understandable document. Instead, the first draft policy should be written by a single technically-competent individual, who has good writing skills, and is familiar with the organization's business activities. If a single individual, who may be on the Development Committee, will be responsible for writing the first draft policy, a Development Committee can be most useful. In this case, the Development Committee can be used for such things as identifying the topics needing to be addressed, preparing a high-level outline, identifying the ways that the policy will be communicated, and providing editing suggestions.

In the absence of either of the two committees mentioned immediately above, special early review cycles with the Internal Audit, Human Resources, and Legal Departments are highly recommended. These departments are important allies of the Information Security Department and will be called upon to enforce an information security policy. If a draft policy does not have the blessings of these departments, it is unlikely to be taken seriously after it is issued. For this reason, some conservative policy writers will meet with senior members of these departments prior to writing a first draft policy, just to ensure that everybody is in agreement about what should go into a policy document. Such meetings can take place even though representatives of these departments are found on one or both of the two committees previously mentioned.

While preparing new or substantially modified information security policies, the policy writer should make sure that an adequate enforcement process exists or soon will exist. If policies cannot be enforced they will, in all probability, not be effective. To have policies that are not enforced may be worse than not having policies at all. This is because the policies may teach workers hypocrisy and tolerance for inappropriate behaviors. Having policies that are not enforced may also lull management into thinking that information security problems have been addressed when the reality is something else.

Management often believes that workers will naturally behave in a manner that is in the best interests of the organization. This is a dangerous and ill-advised assumption. Although policies are unlikely to affect the personal values of workers, management uses policies to give workers the opportunity to conduct themselves in a manner consistent with organizational values. Policies tell workers what is expected of them, that is if they want to continue to have a job. Assuming there will always be a variance between personal values and organizational values, policies will be taken seriously only if effective compliance mechanisms are in place.

In advance of the issuance of new policies, the policy writer should be sure to discuss the ways to achieve compliance with the Internal Audit or Information Technology Audit Department. These might include compliance-checking tools such as software license management systems. The policy writer should also consider the difficulty and advisability of conducting periodic manual compliance check efforts. The manner and means for the accomplishment of these compliance checks also should be envisioned in advance. Human resources policies, such as a disciplinary process and an employee performance evaluation process, will need to be discussed in advance of writing information security policies.

Compliance in many instances can be assisted when computerized tools are used to assist the user. For example, at some organizations, management-approved non-disclosure agreements (NDAs) can be found on an intranet server accessible to all employees. Whenever an NDA is needed, a user can simply print the relevant form found on this server. The ready availability of tools such as this will help users translate information security policies into action.

Policy enforcement need not be painful. Consider using special procedures to make a point. For example, if confidential information is left on top of a desk, the information can be taken and a receipt provided indicating how the worker can retrieve it. The second time confidential material is left out, the worker and the worker's manager both must retrieve the information. The third time requires the worker, the worker's manager, and a vice president. A fourth time could be reason to discontinue the worker's employment.

Enforcement actions are often more effective if workers have are aware of what activities would be information security policy violations, and exactly what penalties would be encountered if they were caught. Establishing clear expectations through an information security awareness program is a very important part of an

effective and enforceable set of policies. Such awareness programs might, for example, clearly state that business information is the property of Company X, and that it must not to be copied, modified, deleted, or used for unintended purposes without management approval.

As a general rule, the policy writer should attempt to guide workers and positively influence their behavior. It should not be the intent to catch people and then discipline the offending workers. While punishment should be used for offenders as necessary, it is not the intent of enforcement mechanisms to generate large numbers of out-of-compliance notices. If a large number of people are out-of-compliance, this is an indication that the policies and related awareness programs have been ineffective. In these situations, the intention behind the policies may need to be communicated more effectively, or the policies may need to be modified to better reflect the organizational culture or prevailing operating circumstances.

## Automating Policy Enforcement Through Policy Servers

At many organizations, the complexity of information systems is overwhelming the ability of staff to manage these systems. To deal with this complexity, new expert systems tools are being introduced. For example, some firewalls include an expert system that will tell the person doing the installation whether a configuration inadvertently has created a serious security vulnerability. To deal with this increased complexity, organizations will need to have more centralized network management systems that play an increasing array of information security roles. For example, network management systems can, and in some organizations do, act as a conduit for the relay of intrusion detection information to a network operator on duty.

An interesting new development along these lines is called a policy server. Policy servers take organization-specific policies and code them in a special machine-readable language that then can be accessed by a wide variety of operating systems, access control packages, and network management systems. Examples of these policies or rules include the minimum number of characters in a password, the maximum number of logon attempts before a connection will be severed, and whether attachments to electronic mail files will be passed through firewalls. In many ways a policy server is expected to be like an active data dictionary because it will be called upon to provide definitive instructions from a centralized point. In the near future, suites of

products from a single vendor, and suites from a combination of vendors, will start to perform some of the rationalizing and centralizing tasks of a policy server.

To prepare their organizations for these upcoming developments, the policy writer should consider how the policies he or she develops today will be put into the computer models of tomorrow. Attempts should be made to be as logical and straightforward as possible. Not only will this help the readers understand how to behave when it comes to information security, but it will also help tomorrow's programmers in their efforts to create computer-enforced rules. Attempts also should be made to achieve the most cross-organization, cross-network, cross-system, and cross-platform coordination of information security policies. This will also reduce complexity and permit the organization to more readily adopt new policy enforcement tools.

## POLICY DEVELOPMENT TIME LINE

---

Before one embarks on an effort to write and obtain management approval for information security policies, it is advisable to clarify who is responsible for issuing and enforcing policies. Only when a clear assignment of responsibility for information security policies exists, should a policy development effort be initiated. Often this means that a centralized information security group mission statement should be prepared and approved before a policy-writing effort gets underway. If responsibility has not yet been clearly assigned, this should be the first step in a policy development effort. If this important step is ignored, the policy writer should be prepared for a barrage of internal politics that is likely to significantly delay the policy writing progress.

Another necessary prerequisite for successfully writing information security policies involves management's perspective. Only after management appreciates that information itself has become a critical factor of production will information security be recognized as a serious matter deserving their attention. This perspective is known by a number of phrases including "information resource management" and "recognizing information as an asset." Management must realize that they are responsible for managing information itself. Historically, management thought information was used only to manage other resources such as people. Management must appreciate that new tools and techniques are needed to manage information itself. In the midst of this discussion, it is appropriate to mention the significant contribution that policies can make. If management does not understand how important information is to their organization, they will be unlikely to support

The future of automated policy harmonization efforts can be readily seen in P3P (personal privacy preferences criteria) which is a multi-vendor standard now incorporated into various browsers including the Microsoft's Explorer. P3P automatically determines what personal information a web surfer will disclose to a remote Internet business in order to obtain further information or enter into a transaction. Both the surfer and the remote business determine what they are willing to do, and what they are not willing to do, in advance of the time when the software automatically negotiates a way to handle private information that is acceptable to both parties. By answering automated P3P questionnaires, both the end user and the merchant devolve their privacy policies into code, and then this code establishes a real-time handshake at the time that a purchase or some other transaction takes place.

information security policy writing efforts. For more information about this topic, see the section entitled "[Policy Objectives And Scope](#)."

Management should acknowledge that there is an information security problem, and that policies are required to address this problem. This must occur before a serious policy writing effort is initiated. While this may appear to be obvious, many well-intentioned policy writing efforts have gone nowhere because the necessary groundwork had not yet been established. This groundwork often includes a brief awareness presentation delivered to top management. Topics at this presentation can include risks that the organization faces, the organization's loss history, incidents suffered by other organizations in the same industry, and generally accepted approaches for dealing with these risks and incidents (such as a policy document).

Ideally, a policies development effort should be initiated after the performance of a comprehensive information security risk assessment. The risk assessment should indicate, perhaps only in high-level terms, the value of the information, the risks to which this information is subjected, and the vulnerabilities associated with the current way of handling this information. A risk assessment will provide useful background information that can be used when selecting appropriate policies from this reference work. The general threat types faced by the organization and other general background information from a risk assessment, may also be included in an information security policy document introduction or preface.

One of the best times to develop an information security policy is when an information security manual is being prepared. Because a manual is distributed widely throughout an organization, it is an excellent place to put information security policies. Specific written policies also may be prepared just before compiling the material for user training and awareness efforts. Perhaps most common amongst these efforts are presentations delivered for new-hire orientation. These efforts may also include a videotape, lectures, posters, or articles in an in-house newspaper. For more information on developing security policies, see Appendix D, “[List Of Suggested Awareness-Raising Methods](#).”

Another good time to prepare policies is right after a major information security breach, an unfavorable computer-related audit report, a security-related lawsuit, or some other type of loss that receives extensive top management attention. This is a good time to move ahead with policy development efforts because management, at these times, is especially supportive of and concerned about information security. It is important to work fast to get management approval at these times because management’s level of concern declines rapidly.

To provide direction for the preparation of other more specific information security documents, policies should be prepared early in the life cycle of an information security effort. These documents include architectures, standards, guidelines, procedures, and contingency plans. An initial set of policies is typically brief, and is

later followed by more detailed policy statements addressing specific areas of concern. More detailed policies would for example include telecommuting policies, Internet policies, and user application development policies.

A good objective to keep in mind when writing policies is that they should be written so that they need not be modified for three years. Because things change so often in the information security field, policies will often be modified only a year or two after issuance. To prevent policies from quickly becoming out dated, policies should be written that are independent of specific commercial products, vendors, and organizational structures. Being independent of these factors does not preclude the insertion of general statements addressing these areas in a policy document. For example, the need for dynamic passwords is often articulated in policy documents, but the vendors and products used to provide dynamic passwords are not generally found in these same documents.

Given the very-fast pace of changes in the information security field, the policy writer should attempt to get management to agree in advance that time will be set aside to rewrite the policy document a year or two in the future. In recognition of the need to keep updating information security policies, this guide is also periodically updated. If you are using an older version of this guide, you may wish to contact the publisher to inquire about the availability of a more current version.

---

## POLICY DOCUMENT LENGTH

---

### Determining An Appropriate Number Of Policies

To be effective, information security policies must be tailored to the unique needs of an organization. Some organizations have many policies, while others have only a few. For example, the information security policy manual at one leading telephone company is over 150 pages, at a large aerospace company it is 75 pages, and at a well-known railroad, it is 25 pages. While range in the number of pages across organizations is quite wide, the trend is clearly to have more detailed and therefore longer policy documents.

While industry category is a critical determinant of the number of pages in a policy document, so too is management’s view of centralization of the information security function. If local management discretion is valued and encouraged, the policy document generally

will be less detailed and therefore shorter. If centralized control is valued and encouraged, then a policy document generally will be more detailed and therefore longer. Most organizations have a combination of these two, where certain information security activities are managed in a decentralized fashion, while others are managed in a centralized fashion. For example, local information security coordinators may handle user ID issuance and password resets at a departmental level, but centralized information security staff may be used for network security matters such as firewall systems administration.

Some management teams will think it is appropriate to be clear about information security matters. In these cases, there may be a need for many policies. Other managers are reluctant to have many policies, preferring to stress reliance on the professional judgement of workers. Still other managers want to keep a document

brief because they fear that workers will get the impression that they are not trusted. But the policy writer should not be shy and overly concerned about minimizing the impact on corporate culture. There are some basic information security requirements that must be communicated by policy, and those should be included in a policy document even if they will provoke difficult questions like the appropriate level of trust in workers.

The audiences to be addressed may be highly-literate, such as at a research institute, in which case more written material may be appropriate. The audiences may be marginally literate, such as a manufacturing organization that employs immigrants from countries that speak a different language. In the latter case, more videotape and graphic presentations of policy ideas may be appropriate. Likewise, an organization may be accustomed to documenting internal business processes, in which case more policies will generally be appropriate. On the other hand, an organization may have deliberately chosen to keep documentation at a minimum, in which case fewer policies will generally be needed.

Although a concise set of policies is more likely to be completely read, there is much to be said for a comprehensive set of information security policies. For example, an employer will find it easier to defend itself in court against employee charges of privacy invasion if the relevant policies were clear and explicit. More importantly, a comprehensive set of policies provides definitive guidance for workers. Definitive guidance in the form of a long policy statement can be quite useful in a court of law where there is need to demonstrate that management has been diligently addressing information security. Longer policy statements are also helpful with disciplinary actions because they explicitly define expected behavior patterns.

Another factor affecting the length of a policy document involves management's expectations for a high-level or a low-level policy document. A high-level document would typically define some worker responsibilities and a few major control measures such as a data classification system. A low-level policy would typically get into much more detail, and may make reference to both tasks, technology, and procedures. If guidance has not been received from management on this point, be sure to clarify this area before actually preparing a policy document outline. It may be a mistake to assume that the information security policy document should be at the same level of detail as other internal policy

documents because in many cases information security is considerably more complex and needs to be discussed in greater detail.

Internet and intranet technology is also altering the appropriate length of policy documents. In the past, policy documents were sent to workers typically in the form of paper memos. Now policy documents can passively reside on an intranet server, and can be accessed whenever workers need the information. This means that documents can be more detailed than they were before without imposing any additional burden on workers. Likewise, the hot links that this technology provides facilitate the establishment of interconnections between documents, which permits users to more quickly locate material of interest. These new technologies allow policy documents to be considerably more detailed than they were even a decade ago without imposing much if any additional burden on users.

One overall strategy to minimize the length of a policy document involves mentioning only prohibitions. With this strategy, readers of a policy document will hear primarily about what they should not do, not so much about what they should do. There are exceptions to this overall rule. For example, workers should report security incidents to someone who is in a position to take appropriate action. This is something that workers should do, not what they should not do. But in general there is merit to this strategy. With this strategy, document length can be minimized because the set of prohibitions is considerably smaller than the set of actions that workers are supposed to perform. Because it involves only minimal instructions, this strategy can also provide flexibility as business activities change.

As a general principle of policy writing, it is wise to issue only those policies that are absolutely needed. This is because people are inherently different, as are the groups that they form. To have only those policies that are absolutely needed permits personal initiative, creativity, and expression to be manifested. Although humans have a tendency to generalize and standardize, this is often taken too far. An example would be an organization that has so many security policies and procedures that they interfere with getting the work done. With this in mind, consider selecting a minimum set of policies that will then be issued on an organization-wide basis, then leave the rest up to departmental, divisional, and other local management.

Rather than starting out with a comprehensive effort, it is best to focus on only the essentials, producing a relatively slim and concise policy statement. Then, as circumstances warrant, add additional policies. This

approach often takes the form of separate policy statements addressing problem areas such as electronic mail and telecommuting. Because it asks for a smaller number of concessions at a particular point in time, this phased approach is also much more likely to get management approval and user compliance. Both the visibility and the good reputation of an information security effort are more likely to be maintained at high levels with such a phased approach because it forces the policy writer to obtain frequent approval and feedback.

The best way to protect information and information systems will always depend on the circumstances. Factors like the type of users, the computer equipment configuration, and the sensitivity of the information will dictate what should be done when it comes to information security. Although some people would like it to be otherwise, policies can never define the true and optimal path for all situations at all times. An open mind and a willingness to deal with the circumstances will go a long way toward finding workable information security solutions. An exhaustive set of policies that denies the reality of each situation, and that denies personal responsibility, is bound to suboptimize information security, if not generate rebellion and disdain. Try to write policies that provide minimal guidance, yet permit situation-specific responses to the truth of the moment.

Another way to look at the appropriate number of policies involves the intention to make information security as user transparent as possible. The more information security is made user transparent, the more likely it is to be accepted. The more user transparent it is, the less the need for written policies. Policies in large measure address areas where vendors do not yet have user transparent automated solutions. These areas are where we must rely on users and other workers. When vendors provide sufficiently reliable user transparent cross-platform security solutions, there will be a significantly reduced need for written policies. That ideal world is many years away, so in the meanwhile a good number of policies will continue to be necessary.

The number of policies to prepare is also a function of the involved audiences. Many organizations prepare several information security policy documents. For example, separate documents might be respectively compiled for users, management, and technical staff. Many of the policies in each of these documents will be the same, although the degree of detail, the technical words used, and the number of examples will generally vary from one document to another. If the audience is composed of end users, the number of policies ideally should be limited to several pages. For a management audience, there will be additional considerations, such as

legal matters, and this is likely to expand the number of policies required. A set of policies for technical staff will most often be longer, more technical, and more detailed. To assist with this audience-related segmentation of policies, following the commentary for each policy found in the next chapter of this reference, the policy writer will find an audience designation.

Another factor affecting the number of policies needed is the degree of security required at the organization. As a broad and general indicator, the more information intensive the activities of an organization, the higher the need for security. For example, a bank will have many information security policies, whereas a chain of coffee shops will have few. Involvement in especially sensitive activities such as human life support or national defense will also raise the need for security policies. An organization with low level security needs, such as a car-wash company, will generally have fewer policies, just as it will have fewer implemented information security measures. An organization with significant security needs, such as an insurance company, will generally have more policies, just as it will have more implemented information security measures.

Although primarily commercial and civilian-government in their orientation, most the policies listed in this reference are applicable to any organization. There are some policies that are relevant only to organizations with certain levels of security. At the end of the commentary section for each policy found in the next chapter there is an indication of the environment where this policy would best be used. A "High" level would correspond to a telephone company, a commercial bank, or a government agency. A "Medium" level would correspond to a manufacturing firm. A "Low" level would correspond to a retail store chain or a car wash chain.

## Determining Policy Length

Beyond the number of policies, consideration should be given to how long each policy should be. To help ensure clarity, the policies appearing in a policy document should, wherever possible, be deliberately kept to a single sentence. The policies appearing in this document are deliberately kept to a single sentence. This concise statement of policy fosters acceptance by workers because it is both easily read and understood. Keeping policy statements concise also emphasizes that policies provide overall guidance, not the details about handling every conceivable circumstance. The details typically appear in information security standard documents and standard operating procedure manuals.

Another policy length consideration is that they need to be specific enough to be clearly understood and consistently interpreted. At the same time, policies should not be so specific that they eliminate an opportunity for local management to tailor them to local conditions. For example, management may issue a policy that specifies that all users must have passwords that are difficult for unauthorized persons to guess. This policy gives local management the latitude to determine whether they want to use system-generated passwords, or whether they want to permit users to choose their own passwords, perhaps accompanied by a mechanism to ensure that users are doing a good job.

The length of each policy is a reflection of how many options management wants to specify. For example, management can specify that it is sufficient that all connections to an internal network must have a firewall or another approved access control system, or can include what type of a firewall will be used, such as a packet-filtering firewall or an application-filtering firewall. Management also can include a definition of the services that will be permitted through the firewall. Generally, it is advisable to keep the policy statements relatively high-level, and to deal with the details, such as those described in the last two questions, in a standard or other supplementary document. Not only will this mean that the policy will be approved more quickly, it will also mean that the policy will not need to keep being modified as the circumstances change.

For those policy writers who feel they must produce a policy document with great specificity, the possible options should be identified and evaluated before the policy is written. Reviewing all the options for every policy with management generally results in an extension of the project far into the future. Instead, an expedient way to proceed would be to have the technical decisions made by a small group of employees, perhaps an Information Systems Management Committee. For each controversial policy, the small group can then prepare a list of options, with an indication of the pros and cons. This list can then be taken to top management for a brief discussion and pre-approval. This approach can significantly increase the likelihood that the final policy is approved because controversial points have been pre-sold with these supplementary lists and associated discussions.

Some organizations may wish to provide specific examples that clarify policies, although it significantly expands the length of each policy statement. As an illustration of this approach, a policy that prohibits the personal use of Company X information system resources could be followed by examples discussing

Internet game playing or the use of the organization's telephones for socializing. Examples make a policy real and tangible rather than abstract. Examples also significantly reduce errors in the interpretation and application of a policy. At the same time, examples may appear to the reader to be demeaning, redundant, and unnecessary. In most cases, examples are not provided with policies except in those circumstances where confusion or disputes are expected.

Another important part of a policy document that may also affect its length, involves explanations of the intentions for policies. If they are going to support information security policies, workers will need to understand why policies are important. The amount of material needed to convey the intention for policies can vary considerably based on the audience involved. As information security is increasingly discussed in the news media, the general public is coming to appreciate what the risks are. This means that the need for words explaining the intention behind a policy document is markedly decreasing. Just in case it is needed, the overall intention for each policy can be found in the commentary section after each policy in the next chapter to this guide. In many organizations, intentions are communicated by in-person training sessions, computer based training software, or some other means besides a written policy.

Other parts of an information security policy document that are not mentioned above, but that may make a significant contribution to the size of a document include a statement of purpose, table of contents, index, glossary, an information-security-related organizational structure chart, statement of information security responsibilities, list of relevant internal documents, risk assessment methodology description, set of information systems security standards, set of information security procedures, history of document revisions, and a case study indicating how the material should be applied. The specific materials to include in a policy document must be determined by the needs of the organization, the organization's sophistication in the information security area, the documents that have been released already, and the responsibilities of the group preparing the policies. An information security policy document that includes all of the above-mentioned supplementary materials can be lengthy, for example 100 pages or more.

## Iterative Development Process

If a more comprehensive set of policies is required, a two-step process is recommended. The first step involves obtaining management approval for a generalized set of

policies, and the second step involves approval for a more specific set of policies. The generalized set of policies could include only 30-50 policy statements as found in the next chapter of this reference. The specific set could include another 50-150 policy statements as found in the next chapter. An example of a generalized policy would be the need to positively identify all users prior to giving them access to internal systems. An example of a specific policy would be the need to use identity tokens that generate dynamic passwords whenever a user connects to an internal network through an external network like the public switched telephone network. In order to be able to accommodate both situations, the policy writer will find both general and specific policies in this guide.

A two-step process is also advisable because it permits the information security group to initially focus on fundamental conceptual models, such as information ownership and data sensitivity classification. After these conceptual models have been emphasized with an initial policy document and communicated through a basic information security awareness program, more detailed requirements can be expressed in a another more detailed policy document. Whether or not this two-step approach is employed, the fundamental conceptual models on which the policies are based should be identified. These conceptual models also should be included in the policy document or other material previously communicated to the relevant audiences.

As discussed in the prior subsection entitled *Determining An Appropriate Number Of Policies*, the policy writer is well advised to take an audience-driven approach to policy development. Policies can generally be divided into those for end users and management, and those for programmers, systems designers, and related technical people. In keeping with the two-step policy development process, the first of these audiences may be addressed in an initial policy development effort, while a subsequent effort could address the second audience.

If the initial set of policies sent to management is too long or severe, management is more likely to reject it. As a result, the window to get policies approved may be closed for a certain period of time. The first set of policies should be kept brief and be relatively easy to comply with. Later, when the first set has been endorsed and implemented throughout the organization, a more comprehensive and more stringent list of policies can be prepared. It is far better to proceed relatively slowly with a series of policy development phases, in a manner that has credibility and frequent management communica-

tion, than it is to prepare a single giant policy document that is then rejected because it was perceived to be too much, too fast, and too soon.

Policies should be written with the classic trial-and-error strategy for dealing with complex problems. After a brief policy has been issued, effects of this policy should be observed, including user reactions and problems with compliance. The undesired effects should be corrected by issuing new or modified policies. The effects of these corrections should be noted, and again corrected for undesired side effects. This process continues as the organization becomes progressively more sophisticated in its approach to information security.

Policies should be reviewed periodically, at least annually, to ensure that they are relevant and effective. It is important to eliminate policies that are no longer applicable. Efforts to streamline policies will be appreciated by both management and users. These efforts also improve the credibility of the information security function within the organization. Workers will appreciate that the information security staff is not out to establish a bureaucracy, but is instead focused on establishing the minimum controls needed to protect organizational information assets.

Delays associated with the information security policy approval process are understandably frustrating for the policy writer. Although the policy writer may have done a respectable job developing policies, management often takes a long time to review and approve them. Policy writers must be patient. Even though information security is regularly discussed in daily newspapers and on television, senior management at many organizations does not understand it. While waiting for policies to be approved, newspaper clippings and other evidence of the need for policies can be submitted to management. This will keep the topic alive in the minds of management and also keep reinforcing the need for management attention to information security matters.

## Table Of Contents For Typical Policy Document

The actual sections of a policy document will vary considerably from organization to organization. This should be a reflection of many organization-specific factors such as the sensitivity, value, and criticality of the information to be protected. The nature of the systems involved, the business activities performed, the local laws and customs, and other factors also should be considered. In many organizations, there will be several

documents, each prepared for a different audience. For more information about creating a policy document, see “[Preparing A Coverage Matrix](#).”

The possible models which can be used as the basis for a table of contents are found in [Table 2-3](#) below. Each has pros and cons, but the policy writer should ask him or herself which most closely matches the way the organization thinks about information security. The policy writer should also ask which will allow readers of the document to most quickly locate topics of interest, as well as which will enable the document to be expanded in the years ahead. While duplication should be avoided, no matter what model is chosen as the backbone (table of contents) of a policy document, there will inevitably be some redundancy.

The typical sections in an information security policy document are: a definition of information security, a statement of management’s intention to support information security, and a definition of general management and specific organizational responsibilities

with respect to information security. Also included will be the specific policies themselves, perhaps with examples or explanations. Some policy documents may include a discussion of the compliance review and disciplinary processes. Mention of the ways to report or otherwise handle out-of-compliance conditions may appear. A list of related in-house documents is also helpful for those who want more information.

Although rare, a table showing the circumstances when certain policies apply is of considerable assistance to readers of a policy document. For example, when a document containing sensitive information is to be sent through traditional mail, policy A would apply, but when it is sent by a trusted third-party courier, policy B would apply. For more information about such a table, see Chapter 17, entitled “[Sample Data Classification Quick Reference Table](#).” These tables can be formatted as decision tables. Rather than making reference to specific policies, a decision table could contain numbers that reference sections of the policy document.

Table 2-3: Policy Document Models

| Policy Document Model                   | Document Focus  |
|---|---|
| Information attribute focus             | Confidentiality, integrity, and availability                            |
| Information ownership and custodianship | Roles and responsibilities  |
| Reader employment status                | Employee, contractor, consultant, temporary, business partner, customer |
| Job title                               | System administrator, systems developer, user, manager                  |
| Data classification                     | Information sensitivity   |
| Required time to restore scheme         | Data criticality  |
| Information valuation                   | Internal information value, replacement value, and value to others      |
| Threat types                            | Legal or business oriented  |
| Equipment types                         | Mainframes, and personal computers, personal digital assistants, etc.   |

Table 2-3: Policy Document Models (Continued)

| Policy Document Model           | Document Focus  |
|---------------------------------|---|
| Geographical location           | In the office, at a client location, on the road, in a foreign country, etc.              |
| Domains of a trust on a network | Different controls within different domains, each of which has a different level of trust |
| Decisions people face           | How often to backup and how to prevent virus problems                                     |

## Which Topics To Address First

For an organization just beginning an information security effort, the complexity of the information security field can be overwhelming. To make it easier for users, management, and other groups who may not be familiar with information security, only a few essential policies should be issued in the beginning. Later, as understanding and support build, additional policies can be issued. For an example of this initial type of information security policy statement, see Chapter 4, entitled “[Sample High-Level Information Security Policy](#).”

Rather than simply copying the policy appearing in Chapter 4, “[Sample High-Level Information Security Policy](#)” consideration should be given to which topics most need to be addressed. Different for each organization, these are the topics that should be addressed in the initial policy statement. These topics typically will include, as a minimum, the responsibility for information security, computer viruses, information backup, contingency planning, system interconnection, user identification, and system access control privileges.

Another way of looking at an initial policy statement is that it should establish the foundation for a successful information security effort. This foundation or organizational infrastructure includes policies, standards, and responsibility statements, and was covered in “[Assuring The Proper Implementation Of Controls](#).” An initial set of policies can be used to establish or clarify missing parts of an information security organizational infrastructure. For example, if enforcement mechanisms are missing, the initial set of policies can discuss responsibility for compliance checking and penalties for non-compliance.

If an information security policy document already exists, the challenge will be to determine what new and changed policy ideas need to be addressed in a new policy document. One of the fastest ways to make this decision is to use a coverage matrix as described in “[Preparing A Coverage Matrix](#).” In this case, the existing policy document can be laid out in a coverage matrix, and the reference numbers of those policy ideas that need to change can be underlined or circled. Next the matrix can be populated with additional policies from this guide, and an outline for the new document can be prepared.

---



---

## POLICY USAGE

### Intended Target Audience

The policies provided in this guide are directed to one who is computer literate and working in a position related to information security. These assumptions permitted the definitions for many common computer and communication system terms like “Internet service provider” to be omitted. To the extent possible, acronyms, and technical computer and communication system terms have been deliberately avoided because

policies must be approved by management, who may not have extensive computer backgrounds. General users are often unaware of technical terms.

### Policy Customization Specifics

The policies in this guide should be reviewed and compared with the policies in place at the policy writer's organization. Using any word processing package, the policies that appear relevant may be extracted using cut-and-paste commands, and placed in a separate

computer file. This new file can then be modified to reflect the unique circumstances prevailing at the organization in question.

Throughout this guide, the term "Company X" is used to refer to a generic organization. This designator is just a placeholder for the organization's name. In spite of the apparent private sector bias, these policies are also relevant to, and have been successfully used by civilian government, military, and non-profit organizations. Similarly, use of this term does not imply that the policies in this guide must be used on an organization-wide basis. It may be appropriate for these policies to be applicable to a subsidiary, a division, or a department. Nevertheless, whenever possible, to keep long-run administrative, enforcement, and related costs down, the widest-possible applicability of the policies should be sought.

The policies in this guide are deliberately written in generalized terms. For example, many policies are equally applicable to diskless workstations, personal computers, super-servers, minicomputers, and mainframes. Rather than restricting a policy to only one type of computer, a generalized policy is preferable because it fosters uniform protection of information no matter where it resides, no matter what technology is involved, and no matter what form the information takes. Accordingly, the policy writer should use key word search terms that are general, such as "network," rather than narrow, such as "local area network." The policy effort should be simplified by taking a platform-independent perspective and creating a set of policies that applies to all computing environments. Taking a hardware and software independent view will additionally help prevent the need to update a policy document when a computing environment changes.

The policies in this guide generally take a most stringent position with respect to information security. For many environments these policies will be too severe. The policies in this guide should be deleted, diluted, or modified to suit the needs of the organization in question. The strong form was stated throughout this material because it is much easier to soften a strong policy than it is to bolster a weak policy.

## Using Key Word Search Facilities

One of the most useful features of this guide and its accompanying CD-ROM is the ability to employ a key word search to locate policies of interest. If the organization is concerned about a certain topic such as viruses, using the CD-ROM search option with the character

string "virus" will identify all areas in the material where the word "virus" is found. The CD-ROM contains all of the information found in the hardcopy guide.

When key word searches are performed, the policy writer should be sure to use the most critical characters only. For example, if one is interested in networks, use the singular version of the word "network" rather than the plural. This will locate both the singular and the plural versions and related terms like "networking." An attempt to search with the most significant single words in a phrase rather than all of the words in a phrase is recommended. For example, the policy writer should search using "diligence" when looking for "due diligence."

Key word searches should also use synonyms. For example, if searching for information confidentiality matters, the policy writer should use "confidentiality," "secret," "restricted," "internal use only," "private," "proprietary," "access control," and related terms. Be sure to search for all the synonyms that describe the area of interest. If the area of interest is unfamiliar, ask someone who knows about it for some key words. In order to make it most likely that all relevant material will be found, generally accepted terms used in both technical publications and general business publications are used throughout this guide. To the extent possible, non-technical terms have been used if the essential ideas behind a policy could be concisely communicated.

Another tip for searching the CD-ROM involves the use of truncated rather than full words. For example, by searching for "copy" rather than "copyright," more policies relevant to the topic of interest will be found. If the search includes a verb or a noun that has irregular plural forms, or that has letters at the end of the word that change, it may be appropriate to initiate several searches, each with a different form of the word.

In an effort to be all encompassing, achieve consistent approaches to information security, and simplify the already-too-complicated life of people in the information security field, the policies in this guide have been prepared with general rather than specific terminology. For example, rather than using terms like "local area network," "gateway," and "router," more general terms like "network" have been employed.

Useful policies may be found in other subsections of Chapter 3 beyond those sections that seem most relevant based on a brief examination of the table of contents. It is important to examine sections in the guide beyond those that seem to directly address the area of interest. Suppose the policy writer is concerned about theft of

sensitive information in paper form. If the policy writer searches only those policies appearing in the “[Physical And Environmental Security](#)” section, then important and relevant policies will be missed. For example, policies addressing the destruction of information would not occur in the section that is mentioned immediately above.

## Policy Organization

The policies in this guide have been organized based on the International Standard for Information Technology—Code of Practice for Information Security Management, generally known as ISO/IEC 17799. This hierarchy is intended to permit easy access to a large

number of policies relevant to a topic of interest. This organizational approach also permits quick identification of related policies that may be related to the topic of interest.

Within a section or subsection of the policies part of this guide, policies are organized in no specific sequence. This means that the entire section dealing with the topic of interest should be reviewed when searching for relevant policies. It is important to review the Table of Contents to identify other sections that may be relevant to the topic of interest. The author of this guide additionally recommends that the policy writer examine the suggested references to related policies for further perspectives and ideas.

---

---

## POLICY OBJECTIVES AND SCOPE

### Motivating Objectives

In most organizations, one of the primary assets at risk is information. Recent studies show that, in modern industrialized economies, from 10% to 95% of an organization's assets are now information-handling related. These assets include hardware, software, and other assets used to process information. Information and other assets used to handle information are both addressed by the policies found in this guide. Risks to people, equipment, buildings, land, and other assets besides information are often recognized and addressed in other policy documents, for example in a human resources manual. There is merit to repeating the same topic in multiple places. For example, the need for background checks could occur in both an information security policy as well as a human resources manual.

Classical economic theory holds that the assets or resources required to do business are land, labor, and capital (the latter refers to money). More recent economic theory describes the factors of production as people, money, plant, and materials. As we move further into the information age, we must add information as another factor of production. An introductory paragraph at the beginning of an information security policy should reinforce this fundamental idea.

Another motivating objective involves management's fiduciary duty to conserve and protect assets, and as noted above, information is now considered an asset. This perspective can then serve as the foundation for explicit policies dealing with information security. This

duty of management should be acknowledged in the introductory paragraph to an information security policy. For more information about using these ideas, see Chapter 4, entitled “[Sample High-Level Information Security Policy](#).”

Many policy statements open with a brief overview of what might happen if information security was not adequately addressed. For example, many refer to a number of risks that the policies are intended to address. From a legal perspective, these include sabotage, terrorism, fraud and embezzlement, extortion, industrial espionage, errors and omissions, service interruption, equipment theft, and privacy violation. Another way to view risks is from a business perspective, with reference to business interruption, erroneous management decisions, competitive disadvantage, loss or destruction of assets, improper record keeping, and statutory or regulatory sanctions. It is recommended that all policy statements make reference to a set of motivating risks, however these risks may be characterized. Further ideas for these motivating remarks may be found in [Table 2-3](#) above.

### Operational Objectives

Policies should be tailored to suit the unique operating circumstances found within an organization. This tailoring process can start with policies that are linked to operational objectives. As an example, the following statement of objectives may be used for a set of policies appearing in an information security manual:

This manual provides a definitive statement of information security policies to which all workers are expected to comply. It is intended to:

- Acquaint workers with information security risks and the expected ways to address these risks.
- Clarify worker responsibilities and duties with respect to the protection of information resources.
- Enable management and other workers to make appropriate decisions about information security.
- Coordinate the efforts of different groups within Company X so that information resources are properly and consistently protected, regardless of their location, form, or supporting technologies.
- Provide guidance for the performance of information system security audits and risk assessments.

## Scope

The scope of an information security policy document should be clarified early in the policies development project. Management should, for example, understand that online etiquette or netiquette will not be addressed in this document. The details of a disciplinary process should be found in a human resources manual, not in an information security policy document. Information quality control and information engineering topics should likewise be outside the scope of an information security policy document. Physical security should be included within the scope of a policy document, but only to the extent that it directly relates to information security. In an information security policy, insurance and legal issues are covered only in high-level terms.

Policy documents should furthermore include specific statements about their applicability. A policy statement could, for instance, state that the policies are: (a) applicable independent of the way information is represented (written, spoken, electronic, and other forms); (b) applicable independent of the technology used to handle the information (e.g., file cabinets, fax machines, computers, answering machines, cellular telephone systems, and local area networks); (c) applicable independent of the location of information (e.g., in an office, at a customer site, on an airplane); and

(d) applicable to information throughout its life cycle (including origination, entry into a system, processing, dissemination, storage, and disposal).

Policy statements should indicate who must observe the policies and when it may be acceptable for worker actions or activities to be inconsistent with policies. For example, a policy statement could say that policies must be observed by employees, outsourcing organization staff, consultants, contractors, and temporaries, and these workers must observe policies unless they have received specific permission to do otherwise from a vice president or higher-level manager. This approach assumes that a centralized management group has the authority to dictate policy for an entire organization. Another way to look at the applicability of policies to specific individuals would be to require compliance for all system users. By continuing to use Company X systems, users implicitly, and in some cases explicitly through a window at sign-on time, agree to comply with security policies. It is advisable to be very specific about the audiences for whom the policies have been written.

Writing an information security policy document that applies to an entire organization rather than a specific segment is the most efficient and effective way to proceed. This approach achieves consistency and complete application of the rules defined in the policy document. Although this may be the ideal, in some cases this approach may be inconsistent with prevailing decentralized organizational structures. Having a centralized Information Security Department that issues policy for the rest of the organization is particularly difficult when subsidiaries and partially owned companies are involved. If a decentralized organizational structure prevails, the Information Security Department may instead issue suggested policies that it can then attempt to sell to the management of the other organizational units. In these cases, the scope of policy statements could make reference to the responsibility of the Information Security Department.

Many information policy statements have in the past applied only to the Information Technology Department. While this approach may have been sufficient 10 years ago, current distributed processing systems require that information security policies apply to all system users within the organization. Some organizations are now expanding the scope of an information security policy effort to include suppliers, customers, and other strategic business partners. This very broad definition of the scope of information security policies is warranted by computer systems that include these outside parties as users. Examples of these more-broadly-scoped

systems include electronic data interchange networks, electronic mail used for purchase orders, and electronic commerce on the Internet for example via extranets.

As a matter of principle, each exception weakens security. For example, if an organization adopts a policy stating that all workers must wear photo-ID badges when in the computer center, and then permits top management to ignore the policy, security will be noticeably eroded. Not only will this cause other workers to question whether top management supports the policy, but it will permit unauthorized visitors to wander about because authorized workers may assume they are part of the management team. While current organizational structures, organizational politics, and other matters will often prevent it, the scope of information security policies should include as many organizational units, types of workers, and circumstances, as is feasible.

There should be consistency between the scope of responsibility of an information security group that is preparing policies and the scope of the policies themselves. If a group responsible for information security in a subsidiary company attempted to write policy for the parent company without prior management approval, problems would most likely occur. Often the documented scope of responsibility for those preparing information security policies is more narrowly defined than the scope of the soon-to-be-prepared policies. Given that management support for broadly-scoped policies has been obtained, this is an excellent opportunity for the Information Security Department to expand both its influence and its formal responsibility.

It is important that the term "information security" be clearly defined in a policy document. By its very nature, information security is multi-disciplinary, multi-departmental, and increasingly multi-organizational. Organizations are still having trouble determining where in the organization the information security function should report, just as they have trouble determining the scope of an information security effort. One recommended operational definition of information security is "any activity that protects information and information systems." With this definition, confidential information might be owned by a third party, and be in the custody of the organization, yet it would be within the scope of an information security effort. This broad definition includes paper-based and voice-based information, not just computer- and network-resident information. It is advisable to augment this broad definition with specific mention of activities performed by certain internal groups such as contingency planning,

systems administration, network management, and records management. Other activities should be specifically excluded, such as those performed by the information technology auditing, risk management, legal, and physical security groups.

Another scope-related factor to consider is the time when policies take effect. The policy document should clearly indicate when readers can expect the policies to take effect. Some situation-specific policies go further, indicating when they will expire. For example, if certain security policies were adopted to facilitate business with a third party, those policies may expire at the same time that a contract with the third party expires. In some cases the issuance date for the policy document will precede the effective date by a month or two. This will give management an opportunity to change their systems to be in compliance. Some organizations recognize the fact that frequent changes in their policies are necessary and expected. To this end, organizations may append words to the end of their policy documents indicating that "Company X reserves the right to change these policies at any time without prior notice."

## Handling Non-Compliance

According to current research, compliance with information security policies is inconsistent. A recent survey indicated that only 23% of more than 500 respondents said user compliance is complete or near complete. At the other end of the spectrum, 22% said there was little or no compliance. Non-compliance is a serious problem that undermines the usefulness of information security policies. Accordingly, some time should be spent considering how both compliance and non-compliance are going to be handled.

After policies have been written, workers must be notified that the policies exist and that they are expected to comply. Although outside the scope of this guide, awareness and training efforts are essential to every successful information security policy endeavor. Awareness and training projects should motivate workers to take information security seriously, sell the benefits of controls, and enlist worker participation in efforts to protect the organization's information assets. Studies have shown that if workers are trained shortly after they receive a policy document, they will be more likely to carry on their normal duties in a manner consistent with the newly-issued policy document. For an overview of the various techniques to deliver these and related messages, see Appendix D, "[List Of Suggested Awareness-Raising Methods.](#)"

Inevitably, some people will think that a policy does not apply to them. If certain managers believe they may be out of compliance, it is important to require them to sign a risk acceptance memo. Such memos typically indicate that a manager believes other control measures compensate for the control indicated by a policy, and is willing to assume the risk of being out of compliance. Because the provision of a signature on such a memo is a relatively intimidating and legally-meaningful prospect, many managers will prefer to comply rather than document the fact that they are out of compliance. The prospect of defending an out-of-compliance situation through the risk acceptance documentation process may be daunting and a significant motivation for management to comply. For a copy of a risk acceptance document, see Appendix L, “[Management Risk Acceptance Memo](#).”

Compliance may be fostered by obtaining signatures, either at the time of employment or on a periodic basis. It is recommended that recipients of an information security policy indicate in writing that they have read, understood, and appreciate the implications of the policies. A signature affirming a commitment to comply also may be obtained at the time that a user ID is issued to or renewed by a user. Signatures can emphasize the fact that management takes information security seriously, in addition to providing the organization with specific written evidence justifying disciplinary measures up to and including termination. For an example of a form requiring such a signature, see Appendix J, “[Agreement To Comply With Information Security Policies](#).”

---

## DISCLAIMERS

---

### Need For Customization

The policies provided in this guide are in generic form. They should not be used without customization to a specific information systems security environment. For such customization to be properly performed, the following prerequisites must exist:

- A specialist in information security must be involved.
- The specialist must have a broad understanding of the risks faced by the organization.
- The specialist must understand the controls used to handle these risks.
- The specialist must have a good understanding of existing information-security-related policies, guidelines, procedures, standards, and related material.

To meet these prerequisites, certain background work will need to be performed by the organization seeking to compile an information security document. For example, to meet the second prerequisite, a risk assessment such as a scenario analysis, a quantitative risk assessment, or a standard-of-due-care controls review is recommended. To meet the fourth prerequisite, consider completing a series of interviews with involved parties to appreciate not only what the existing policies mean, but also how well-known the policies are, how well workers have complied with the existing policies, and the costs and benefits the existing policies have engendered.

### Balancing Trade-Offs

Because this reference guide contains a comprehensive set of policies, it should not be surprising if a few policies that contradict other policies are found. For example, freedom of information policies may conflict with right to privacy policies. Each organization will need to determine where this and other lines should be drawn. Workers should be informed of these management decisions lest they be left to make these tough decisions on their own, perhaps with catastrophic results.

Like many activities in the information security field, writing policies involves tradeoffs. Frequently encountered tradeoffs include those between cost and security, speed and security, flexibility and security, and ease-of-use and security. There are many conditions and limits in the information security field, and policies must also be designed with these in mind. For example, a policy dealing with the termination of employees for violating certain information security requirements may be incompatible with existing labor union agreements. Other limits include standard industry practices, prevailing corporate culture, societal ethics, laws and regulations, and the structure of third-party relationships.

The intention of this guide is to provide a wide variety of generally-accepted policies. It is not the intention to have the body of this reference guide constitute a logically-consistent set of policies, although several logically-consistent policy statements are provided at the

end of this guide. The logical inconsistency between some policies is also a reflection of the fact that there is no standard set of specific policies to which all organizations must subscribe. Instead, a set of policies must be uniquely tailored to the requirements of each organization.

## Need For Competent Advice

Many of the policies described in this guide contain specific numbers, time periods, or other information that is technology-, jurisdiction-, or organization-dependent. It is strongly recommended that the services of a computer-literate attorney and an experienced information systems security specialist be retained prior to placing these policies, or policies derived from them, into service. In some instances, such as the

establishment of encryption policies, it also may be advisable to get assistance from a specialist in a narrowly-defined subject area. A review by the Human Resources Manager is also advisable to ensure that the policies are consistent with an organization's existing policies.

Lastly, the material in this guide is intended to provide guidance and ideas for potential policies. It is not intended to provide a specific course of action or a specific set of words for an organization. Some of the suggestions found in this guide will have little or no bearing on the organization, and in some cases these suggestions may even be illegal in the organization's jurisdiction. The material found in this guide should not be used verbatim, but should instead be customized to the specific circumstances at the organization.

