DATA SECURITY MANAGEMENT

POLICIES AND PROCEDURES: THE BACKBONE TO A STRONG SECURITY MODEL

Bruce A. Lobree

INSIDE
Policy Model for the Company; Defining the Standard; Outlining the Standard; Owners, Authors, and Experts; Referring to Other Standards; General Standard versus Technical Standard; Breakdown of the Finished Document; Issues to Avoid; Signatures and Implementation; Audit Trails and Accountability

BEFORE STARTING
You have been asked to write a security policies and procedures manual for your department, or maybe for the corporation. Where do you start, what type of document do you write, and who will own it when you are finished? What industry standard are you going to try to meet, and what is the intent of your document? Is it an audit requirement, a corporate requirement, or did your boss hear at the conference he just attended that having documentation is a great way to improve your company’s security and operational efficiency?

Policies and procedures are sometimes used as standards. These documents are named the same and sometimes mistakenly named inappropriately. For example, while policies and procedures are not standards, there are standards for policies and procedures. Basically, policies define what an organization does, and procedures define how the policies are executed. Standards, on the other hand, define what is used for either policies or procedures. For example, an organization may determine that its policies and procedures comply with BSI7799, a standard; or it may set standards for access control.

Most people today look at these types of documents and think they are training guides that are not really needed until the product or company

PAYOFF IDEA
There is a process to creating effective information security policies and procedures. Knowing and following these steps will ensure that the results are easily understood and followed. This article presents guidelines for developing and implementing policies and procedures.
is in a mode in which employees need training on some function of the operations. In fact, policies and procedures may be the single most effective way to cut costs, simplify training, and identify weaknesses in an organization. If implemented correctly, they can also improve effective control of engineering, quality control, and operational accountability.

This article discusses at a high level several of the key items that one must go through before one can even begin to write these documents. By the end of this article, readers will have a list of items that need to be accomplished before, during, and after their policies and procedures have been written.

Every company has a different model, different forms and different guidelines that must be followed, and some have none at all. For companies having none at all, this should be created before any policy or procedure can be properly controlled. There are some very basic rules to policy and procedure writing. When followed, these will make the author's job considerably easier, as well as all those people who will assume this role when any of the identified persons on the document move on.

No matter what type of document is being written, the author should remember that patience, perseverance, and consistency are the items that will get the final document out. He or she should not shoot too high, but should remember to cover the important issues and clearly identify the controls he or she wants to achieve.

**POLICY MODEL FOR THE COMPANY**

Before writing any policy or procedure, the author of the document must determine several very critical items, including:

1. scope
2. type (general versus technical)
3. intent
4. inclusions
5. participants

Each area must be individually addressed and answered before proceeding further.

**Scope**

You have been told to write a policy for remote access by your boss. Some key questions that need to be answered are discussed below.

**Will this impact the whole corporation or just your department?**

If the intent of the document is to only be used within your specific department, these answers will come quickly, and usually you will already know them. Never presume that your reader knows the same informa-
tion you do; always presume he or she does not and record information accordingly so everyone achieves the same level of understanding needed to be able to comply with the policy. If the documents are intended to be used by the entire corporation, then ownership, signoff, and implementation may have to be at a senior corporate level, which will require a completely different model that involves a broader group of people.

This single determining factor will not only impact the names on the document, but also the methodology of the entire document going forward. For the purpose of this article, assume that a corporate policy is being completed. The purpose of this is that any policy or procedure below this will be similar and, therefore, this same guide can be used to develop the needed controls.

What policy or procedure is being requested? Today’s policies and procedures may be influenced by outside sources or standards. In the computer industry, there are several. ISO9000 is one of the oldest and most defined standards used worldwide. It is very well documented, and the requirements to fulfill it are clearly outlined. For further information, go to the Web page: http://www.isogroup.simplenet.com/. This page not only outlines the ISO requirements, but also provides a basic checkoff list.

One of the older standards is the U.S. military Orange Book, which was part of the Rainbow Series of standards. For more information on these documents, go to the Web page: http://www.radium.ncsc.mil/tpep/library/rainbow/. The Orange Book was the Department of Defense’s Trusted Computer System Evaluation Criteria. This remains the standard used by many companies and industries today.

There is also BSI 7799, which is the new British standard that many companies worldwide are starting to follow. While primarily being used in Europe, it is currently under consideration as an international (ISO) standard. As a result, many American and Asian companies are now looking to come into compliance with BSI 7799 as well, so that they can meet European and ISO standards. For further information on these requirements, go to: http://www.bsi-global.com/Information+Security/index.xhtml.

In this author’s opinion, the most common cause for the creation of any type of standard is a Statement on Auditing Standards (SAS) No. 70, “Service Organizations,” better known as an SAS 70 audit. This single statement from management, “An SAS 70 Audit is going to occur. Can you please prepare for it.” can cause even the most stalwart security techies to freeze in their tracks. The SAS 70 is very vague and leaves much room for interpretation by the auditor. Unlike the ISO 9000 and the BSI 7799, which clearly outline standard requirements, the SAS 70 does not have this clear documentation. A good place to start is with the AICPA Auditing Standards Board to obtain more information.

Read the general requirements for each type of standard before deciding which one to meet. Also find any standards that have already
been put in place in your industry. Finally, having decided what requirement you want to meet and what level of control you want to achieve, confirm it with that level of management to be sure they agree before proceeding further.

**Who will own this document when it is completed?** The answer to this question is easy. The level in the organization impacted by the document will directly determine the signatures needed. If building a corporate standard, then the CIO at a minimum must approve the document. It would be better if the CEO approved along with the CIO; then no one in the corporation would be able to disagree with the implementation of the standard. When writing this type of document, be aware of implementation time and the impact of getting signatures from this level of management.

For a departmental document, one should never go to the CEO for a signature, unless of course the CEO is the head of that department. Signatures from managers and directors are much easier to obtain and will help expedite the implementation process. The lower the level of signature required will directly impact the ability to get the document approved; inversely, the higher the signature level required, the larger the part of the corporation that will be impacted.

Do not use standards for publicity unless you want to be directly associated with them. Security documents are not, in general, career-enhancing documents that will help you achieve a better personal profile, unless you work in a security company where security is the only priority.

**Who will control the document?** This will be determined by whose signature of empowerment is on the document. This is also impacted if the company has a specific department that maintains all policies and procedures and enforces them. In today’s Web-enabled world, many times this is a server that stores all corporate documentation. Access to this server must be tightly controlled and monitored, with individual access recorded.

Each document is signed off when it is completed, and it is the responsibility of the signing party to either own the document or specifically assign that ownership to someone. If this is not done, the document will go into the void of unknown where all uncontrolled documents go and will be of little to no use to the intended group and become obsolete and probably forgotten.

If an audit trail is required, it will be even more important that the document’s author and signing body know exactly the path of control the document will take. The finished document should include this information within the body of the document for later review. This will include
who wrote and approved the document, who owns the approved version, and where updated copies will be recorded and kept.

If electronic signatures are used for the approval process, then these signatures must be kept in the same location as the document for later referral should it be needed. If the signatures are stored in a different location, they can be lost or misplaced, and that could nullify the document in question because proof of approval would no longer exist.

Type (General versus Technical)

There are two basic types of standards: (1) general or non-technical and (2) technical. These types of documents are very different in their intent and final version. They are also treated differently, in that a general standard may change very rarely — if ever — depending on the scope of the document. The technical standard should be a living document that will change every time the environment, system, or program that it covers changes, so that controls and reference materials stay current.

A good general standard will not include technical requirements. This type of standard is intended to be generic and will not include implementation or installation information. General standards will usually not go down to a level of detail wherein the reader will have actual instructions for implementation and may have limited user information. These documents can go from the individual group or department up to and including the entire corporation.

A good technical standard is very specific and will have details on how and why something is implemented. It will include the specific details on each of the controls in question and will allow the reader to install or implement the item that is covered by the procedure or policy. Technical policies and procedures may not cover corporations and are generally only used within specific departments or groups; they are intended for the actual implementation.

Inclusions

Good standards never reinvent the wheel. This means that if a standard for a particular item or configuration already exists, then it will be appropriately referenced. This prevents the overlap of standards and reduces the amount of data a person must read. Before referencing a document, be sure it exists in something other than draft form. All referenced documents should be listed in an index at the end of the document. These references should include title, author, version, and date of revision or creation, as appropriate. This is done so that should particular document controls change, the reader will know when to go to that particular document.

The only time a standard should be repeated is when the pre-existing standard is not detailed enough to either complete the task or else understand the intent of the standard based on the document that is being de-
veloped. Even in this particular situation, the author of the standard should still reference the document that contains the original information.

**Owners, Authors, and Experts**

“He who authors does not own and is never the expert” was a statement this author once heard at a conference. This may not be completely true, but many times it is at least partially true.

The owner of a document is that person who has the responsibility of making sure the final document is accurate and that it is available to the appropriate audience. It is also the owner’s responsibility to maintain version control and number of copies and locations of copies of any document. In the case of a Web-based solution, the owner must ensure that the official copy of the document is only located in one place with the appropriate controls in place.

The author is the person who actually writes the document. Many times, this is a contracted person who may know little or nothing about the subject matter. This person can be a temporary contractor or a senior executive in a business — it does not matter. The only responsibility the author has is to make sure that the grammar is correct and that he or she is not re-creating a document that already exists. The author should always verify all referenced documents and other types of materials.

Finally the experts: they may have limited or extensive knowledge in the area in question. Document owners should never rely on one person’s opinion or testimony as it relates to their standard. Such information should represent a cross-section of the people who have knowledge in the area to be standardized. If a document is to be utilized by an entire corporation, then input should come from several areas of the corporation (if possible). This will help ensure that what is intended is achievable. If there is only one person in the entire company that knows anything about the particular subject, then go outside the company to make sure that the facts are correct. Bottom line: never rely on one person’s input unless the standard in question will only impact that one person.

Be sure to list, within the document, each of the types of people used in the development of the document. This further enables the document to get buy-in from the affected groups.

**DEFINING THE STANDARD**

This is the single, most difficult part of the entire process in this author’s opinion. Defining what the standard will — and most importantly, will not cover — is the first step to a successful document. Each step after this one will be determined by the action taken now. Remember: the document should not be so broad in scope that it is not effective; yet it should cover enough that the reader will understand its intent and will also get enough overall information to achieve compliance.
An example of a document that will always have a broad scope is the corporate security general standard. This document will outline everything — from passwords to access control, forms of user authentication, and project approvals. This document will be very generic in nature, but it will specifically state what documents outline the controls relevant to that section of the standard. There should be no technical information and all data should be appropriate for the targeted audience.

For other types of standards (i.e., dial-in connectivity), there should be a specific scope statement at the beginning of the document that lets readers immediately know if they have what they are looking for. This statement will also define whether the document is technical or general. This does not mean that a general and technical standard cannot be in the same paper — they can.

The title of the document should state what the document is about and what type of document is being written.

Example title: Desktop Application Technical Standard
Example scope: This document outlines the desktop standard application and how applications may be applied for and approved for implementation. This document will outline and supply the approval documentation. It will further clearly outline the process for testing and installing applications on both local as well as remote workstations connected to the corporate network.

OUTLINING THE STANDARD
Now that the document type has been determined, the policy or procedure can be created in a reasonably straightforward fashion (see Exhibit 1). Outlining the document allows for a quick proof of concept to determine if, in fact, all the needed data has been effectively defined. If something is missed, the outline will help identify the additional information needed.

The outline should be reflected in the table of contents and the reader should be able to roughly understand the overall contents of the document. The finished document should flow from beginning to end, starting with the scope and ending with the finest details that the reader will need. The last section of the document should be an index that will allow readers to go back to any individual item they need to know about and understand.

If the document uses complex language that some readers may not understand, be sure to add a definition table at the end of the document. Always try to use the full wording for any acronym before using that acronym. Many industries use the same letters to mean very different
things. For example, ID could mean Information Diagram, Identification, or Internal Data.

OWNERS, AUTHORS, AND EXPERTS
You have been requested to develop a document for dial-in service by the CIO (see Exhibit 2). The CIO is the owner of the document and you are the author. The only way this will change is when the CIO passes ownership on to someone else — probably you. Usually this will be a security person in a managerial or higher level. Either owners are the highest people in the organization who can have responsibility for a document, or they are assigned the responsibility. In either case, the document’s author should have clear direction about the intent of the document before starting, which also gives a defined finished product.

It is the owner’s responsibility to make sure that the level of involvement by each of the three groups of people is appropriate so the author can complete his or her assigned task. There must be sufficient involve-
ment that the finished document will be approvable and implementable; otherwise, everyone has wasted his or her time.

As stated previously, owners, authors, and experts will each have specific responsibilities or duties associated with the final product. Key individuals should be identified in the final document on a separate page that can be used for change control purposes. This single item can save considerable time and make a slow process more efficient. It will allow for quick identification of the responsible individuals and expedite the approval process on the whole. If physical signatures are required, it is also easier to move one piece of paper than a whole document. The document can be placed online for review, and the signature document can be moved either online (allowing for digital signatures) or via land-based mail (allowing for physical signatures).

REFERRING TO OTHER STANDARDS
Common mistakes that people make in writing policies and procedures include referring to a document that cannot be either found or does not yet exist. To the reader, this is more frustrating than trying to implement.
something that has not yet been done. Statements that refer to other documents must always be accurate and properly annotated. Also, it is best to create a complete listing of all referred-to documents at the end of the document in an index, as stated previously.

Secondary to this issue, documents should be approved if they are referenced or at least be in some type of formal format. The reference should clearly state the type of reference (i.e., internal versus external, White Paper versus published book) and further state when the document is expected to receive appropriate approval if not already. Approved documents will always have much more strength in their ability to impact the overall effectiveness of any forthcoming document.

The format chosen to reference documents is whatever is standard for one’s company. This author recommends listing the referenced document in a footnote on the same page, which allows readers to know right away in which document they can find all the supporting information. This, along with an index, will provide readers with a complete and easy-to-use reference list.

**GENERAL STANDARD VERSUS TECHNICAL STANDARD**

A ship can carry a boat, but a boat cannot carry a ship. The same holds true for general or non-technical versus technical documents. A general standard should never contain technical details; however, a technical standard may contain general information when appropriate.

The best way to define a general standard is that this document will have an impact across a broad area. This type of document should try to not contain technical specifications or technical guidelines for implementation. What this document should contain are those roles and rules that will guide the reader through the process of understanding what needs to be done and determining the final goal. A good general standard will allow the non-technical reader of document to understand the intent of what is to be accomplished.

How the reader will get from not being secured to being secured and what specific configurations need to be put in place should be put in a technical standard. Such a document will contain specific instructions that lead the technical reader through the process of configuration and implementation of the product/hardware device in question. Technical standards will contain a high level of detail, right down to the keystroke needed to meet the predefined requirements as appropriate.

**BREAKDOWN OF THE FINISHED DOCUMENT**

Development of policies, procedures, and standards should try to always follow the same path and format within a particular company. They should always have the same structure and be in one language. If, for example, Spanish is the company’s primary language, then all documents
should be written in Spanish first and then translated into the languages employees use if they do not understand Spanish.

The actual content of any standard will change. However, the structure will not change. Below is a very simple breakdown of chapters and the path to be followed.

Section I: Title page, to include:
- department owner's name
- title of document
- revision number
- disclaimer about proprietary nature of document

Revision/document control page, to include:
- all listings of personnel involved in development (owner, expert, author)
- all signatures
- location of original
- revision history

Table of contents

Section II: Introduction, to include defining the type of document and what the intent is:
- Scope: What is the area, system, or objective of this document?
- Justification: Why is this document being written and what will it accomplish?
- Audience: Who will this document affect and how should they be notified or trained?

Section III: Actual standard and information to support policy or procedure, to include:
- controls
- policy
- guidelines
- instructions to implement (if this is a technical standard)

Section IV: Testing and verification instructions to prove standard is being appropriately applied, to include:
- audit controls
- document retention and verification methods
- types of verification requirements

Section V: Any and all supporting documentation, to include:
- reference list
- appendices
- listings
- diagrams
- Index(es)
Not every standard will contain all of these sections or parts. However, a good standard should, at the least, address the majority of these items.

ISSUES TO AVOID
A good standard is never used as publicity or career enhancement for a particular person or group of people. Standards should be used for education and awareness for a particular issue, problem, and solution. Document authors should always be aware of the audience that will be impacted and include them in some form or fashion in the development of the final document.

Not involving the affected group in the development of a standard will make implementation that much more difficult. Change is generally not wanted, and people tend to push back when forced to comply with any particular type of rule. If they help in the development of policy or procedure, then they have a vested interest in the success of the completed document.

Having lead members of the affected group be part of the experts in the development is one way to get them involved without having to put them into the actual signature process. This will allow for the proper identification and association of those people when the document is actually implemented.

Never attempt to use a standard to meet people or put your name in places it normally would not go. Standards should impact the appropriate group. In developing a corporate standard, be sure that management has buy-in to the process before starting. That being done, the audience and the team who will approve the standard have already been defined. This will also avoid trying to impact the wrong audience, which can be a career-limiting move if it includes management but does not have management’s approval.

SIGNATURES AND IMPLEMENTATION
The document is complete. The past two weeks have been spent interviewing, reviewing, rewriting, and correcting the document. Now for the final task in this process: getting the signatures that will empower this document. There is no easy way to accomplish this task and only you will know the best way to go about completing this process. Every person who signs this document may also have a reason for not signing, which is why that person needs to be involved in the entire process.

Some companies have a very specific signoff process that can be followed, but most do not. You may even be the first person in your company to go through this process. Depending on the level of impact of your standard and who the actual audience will be, as stated earlier, will determine who needs to signoff. If it is the CEO or CIO, and you have determined that a physical signature is the way you need to proceed, you
should plan on meeting with him or her to get the actual signature. If the
signature is from a manager, this may not be needed; however physically
meeting with someone is always preferable to an e-mail when a physical
signature is needed.

If a digital signature is going to be used, send the document with a de-
livery receipt and clearly state what you need in return and the desired
timetable. In this way, you will get a response when the reader has
opened the document, and he or she will know exactly what is needed.
This will allow you to send a reminder when the appropriate amount of
time has passed and you have not received a response. Be sure to put
that time frame in your message so the reader is aware of the criticality
of his or her specific actions. If you do not put a time limitation on your
message or do not state one in your meeting, do not expect the signer to
put one in place for you.

Once signatures have been received and the document is ready for
publishing, be sure to go to both the legal and human resources depart-
ments to find out the best way to educate the company, organization, or
department and make everyone aware of the new document.

Most importantly, wherever one decides to store the final version of
the document, be sure to store the signatures with it. If the signatures are
physical, then they will be on the final version of the document, which
should be stored in a safe and secure location. If the signatures are elec-
tronic, then they should be stored in the same directory as the final ver-
sion of the document, and everything should be password-protected so
that documents and signatures cannot be changed without authorization.

AUDIT TRAILS AND ACCOUNTABILITY

The audit trail and accountability represent key parts of the document to
maintain, and yet can be the most unnerving in the long term. Assume
that the document is finished, that all signatures are in place, and every-
thing else is complete. Then there is an audit by an electronic data pro-
cessing (EDP) auditor. Depending on the standard this particular auditor
chooses to use, there may be compliance, or there may not be.

The following questions will be asked: How did you get the informa-
tion out to the target group, and how can you prove it? How do you
maintain the document, and when was the last time it was reviewed?
How do you make new employees aware of this document, and what is
your compliance and verification process? And, where is all your docu-
mentation to prove its authority and controls?

All of this information should be kept in the same location or be re-
ferenced by the original document. This will greatly improve the reliabil-
ity and possibility of passing any type of audit. It will further improve
the viability of the document over the long term as personnel turn over
and others become responsible for the document. Each generation after
the original will be able to follow the paper trail and reconstruct it when needed.

CONCLUSION
A good policy and procedure document is one that can be employed and understood by the target audience. The owner of the document should be able to employ it without going to great lengths and costs, unless the document so requires. The document should be reviewed and verified as being properly implemented. That review process, as well as the ongoing training process, should be documented.

The entire target audience will understand not only the document, but also the reasons for it, even if they do not totally agree with it. There will be a process wherein they can submit any problems or concerns and, as appropriate and on a regular schedule, those changes will be added and conveyed to the appropriate audience.

Additional Reading

Bruce Lobree is currently the head of operational security for Siebel Systems, Inc., where he is responsible for all computer-related security and has oversight of operational physical security. He has more than 20 years of experience in computer systems and networking, specializing in computer security for the past 13 years. He has worked in the manufacturing, utility, financial, and software industries, as well as the ASP business. Lobree has spoken to a broad range of industries about computer and network physical and logical security.