Global Information Assurance Certification Paper

SHELFWARE

How to Avoid Writing Security Policy and Documentation That Doesn't Work

Abstract:

"Shelfware" is an informal term for documentation that is required, but will probably never be used because the intended users don't find it helpful. Anyone who writes security policy documentation should ensure that the result is concise, clear and authoritative. This paper outlines a strategy for achieving that goal, and thus maximizing the chance that the intended users will actually employ the resulting product.

This paper explores the "GIAC Basic Security Policy" material (Part V of the course), looking into pitfalls that can make security policy and similar documentation unwieldy and unreadable.

The Problem – What is shelfware?

All too often, security policy and similar documentation becomes shelfware; that is, it fulfills the organization's requirement that it have a policy, without achieving acceptance as a functional tool. So, if asked, the security manager can say, "yes, I have a security policy" (or contingency plan or incident response plan, etc.), "and there it is on my bookshelf." But when tasked with making a security decision or responding to a crisis, this manager will rely on his own expertise, rather than referring to the written documentation.

This problem is especially evident in large organizations, with standardized documentation requirements. In the United States Department of Defense (DoD), security documentation must satisfy the DoD Information Technology Security Certification and Accreditation Process (DITSCAP)[1], which calls for a main document and eighteen appendices. The result can be a daunting array of binders. If nobody reads them, essential information may be overlooked.

Part of the solution to the shelfware problem is to make the information as focused and readable as possible. But that is a challenging assignment. According to a textbook description, "Technical writing is more like investigative reporting than scientific writing, requiring practitioners to gather information rapidly, identify audiences, and use creativity and problem-solving skills."[2] This is unfamiliar work for many of the technical personnel involved in information system security. Still, in order for the technical message to get through, technical writing skills must be applied.

This paper proposes to solve the problem by focusing on just a few technical writing skills, those that are required to fix the worst readability problems commonly found in security policy documentation.

---

[1] Department of Defense (2000). Department of Defense manual number 8510.1-M: Department of Defense information technology security certification and accreditation process (DITSCAP) application manual [downloadable file]. URL http://web7.whs.osd.mil/html/85101m.htm, p. 120 – 121.

[2] AltaVista (n.d.). Art of technical documentation [WWW page]. URL http://shopping.altavista.com/product.sdc?n=24319&p=10333193

The Strategy – Employ selected technical writing skills to improve security policy documentation.

Manage the document set.

If your security policy will be a multiple-document set (or a main document with a number of appendices), you should start by planning how you will manage the document set. This plan should include:

- placement of content. This is especially important for content that is needed by more than one document or appendix. The Backup Plan, for instance, is something that could be included in a System Administrator's Guide, an Incident Response Plan, and a Contingency Plan. But if you cover system backups in all three places, your policy will probably be inconsistent. Some material will occur in one place, and not another. Some accounts will be more detailed than others. Some accounts of this procedure may actually contradict each other. Even if you start out with the same plan in three places, any document updates risk creating the problem all over again. That is why one of the main database normalization rules is: Eliminate redundant data.
- consideration of anticipated readers. Notably, any material that ordinary users must read should be concentrated in just a few documents. Within a given document or appendix, material should be segregated by reader, as much as is consistent with the flow of the document. For instance, material that is intended for ordinary users should appear under a different paragraph heading (at some level) than material intended for system administrators. Also, material that the reader must know should be clearly distinguished from material that he should refer to, as needed. Help readers focus on the knowledge, tasks and responsibilities that apply to them. For large document sets, a user's guide can make this task easier (see Table 1 for an example).
- naming conventions for key players. One of the reasons people don't use active voice is, they don't know what to call the active parties. If you decide at the beginning that "the INFOSEC Team" is writing the policy, "the System Developer" is writing the code and handling system integration, "the Designated Approving Authority" is judging whether the package is fit for distribution and use … and so on … you can improve both information content and consistency.

Table 1 - Documentation Set User's Guide

Section	End User		Supervisor		Evaluator
	know	refer	know	refer	
System Security Authorization Agreement				✓	✓
System User Guide	✓		✓		✓
System Administrator's Manual			✓		✓
Contingency Plan				✓	✓
… etc.					

Document planning is especially important for documentation efforts that are undertaken by a team. Whether your project is a team effort or a one-man show, you should plan on some give and take. The above planning elements will probably require adjustment as the project progresses and the result begins to take shape.

Do it with style.

Plan the style and tone of your document, as well as its organization. This is also important in a team effort, where writing styles differ. This doesn't need to be an abstract task, because you can get good improvements in readability by focusing on just a few particularly troublesome areas:

- Minimize the use of passive voice, and always identify the active party. If you don't know who the active party is, consider your job incomplete until you find out.
- Consider using the second person in selected documents. "You" is an especially effective and compact way to express many of the requirements found in guides (e.g., the User Guide).
- Determine the most compact convention for third person pronouns that is acceptable to the organization or customer, then stick with it. Many will still accept the use of "he" to designate a person that may be of either sex, because that was a standard English practice until only recently. Or they may accept the occasional substitution of "she" on a random basis, providing the sex stays consistent where it appears to be referring to the same person. Otherwise, you may have to use a less readable form, such as:
  - If a user forgets his or her password, then he or she must ask his or her supervisor …
  - If a user forgets his/her password, then he/she must ask his/her supervisor …
  - If a user forgets ?? password, then (s)he must ask ?? supervisor …
- Substitute "must" for "shall" and "will", where "must" is what you mean. That's a plain English way to avoid inconsistencies in applying "shall" and "will", leave out a distinction that's lost on most readers, and never be mistaken for talking about the future.

Whatever your decision, be consistent on applying these throughout the document set.

Focus on the reader.

Following your document plan, focus on different readers in different documents or sections. Identify the anticipated readers before you write, then stay focused on that audience as you develop your subject. You may find it useful to identify the intended readers at the start of a document or appendix, but it's not always necessary to be that explicit.

In situations where material for various audiences supports a single task or topic, group the material by audience and clearly identify the groups. Paragraph headings work well for this.

Identify the consequences for failure to follow the policy, wherever you can.

Even if you know that your current reader is an experienced professional who doesn't need detailed explanations, write at the level of someone who is relatively new. Explain things as if you were writing for his replacement.

Follow the action.

Focus on the problem at hand. For action-oriented information (e.g., an Incident Response Plan) present the material compactly and emphasize the action. Don't let background knowledge obstruct the flow and obscure the policy. Unless it is very short, separate background knowledge (such as why this is the policy) from the active elements. This kind of material should be presented after the active elements, unless it is clearly required to understand the action.

Keep it short! Think of the reader who only opens the reference to understand one element of policy or one procedure … the one you are writing now … and explain it as briefly and directly as possible. Add amplifying information and conditional sub-procedures at the end.

Use topic sentences, as much as possible. The first paragraph of each paragraph should convey its main idea. Try reading just the first sentence from each paragraph, to check your flow and information content. Note that outline headings typically don't convey complete ideas, so they don't serve the same purpose.

Be careful what you borrow.

If you use a security policy that is already developed, be careful in adapting it or integrating it with your existing material. A number of sources, including GIAC (as part of the course) and the Tech Republic[3] web site offer security policies of various kinds, acceptable use policies, and so on. These are very useful, as examples and reminders (so you don't forget anything). But they can cause readability problems too, especially if you borrow from more than one source. Problems include:

- bad fit. Much of the copied information doesn't apply to the current situation.
- paste-in bloat. Extraneous material and explanations are added, along with the pasted-in material. Desired material (from different sources) is covered more than once.
- disrupted flow. All the essential material may be covered, but it is not presented in logical order, or in a manner that emphasizes the main points and makes it easy to follow.
- style changes. Copied material uses different terminology and writing styles, so the result is inconsistent.

Borrowed material is rarely suitable for pasting in as-is; it usually requires a major editing effort to overcome the problems listed above.

Make sure that bulleted lists have similar items, grammatically.

Bulleted lists are a compact and memorable way to convey information, but they become less readable if the items don't match, grammatically. Typically, the list is introduced by a sentence fragment, and each item in the list is an optional ending for it. So, for instance, if the list starts out as a list of nouns with modifiers, it shouldn't have any items that are verb phrases.

[3] TechRepublic (n.d.). Search results – Tech Republic [WWW page].
URL http://www.techrepublic.com/search/result.jhtml?_DARGS=%2Fsearch%2Fquery.jhtml.5

Be rigorous in using categorizations.

Categorization is a powerful tool for breaking down complex information. Unfortunately, sloppy construction of category sets often makes them confusing. Some common errors are:

- Logical classifications … the kind that divide a something into categories, like cutting the pie … don't account for all pieces of the pie.
- Categories are too broadly defined, omitting important limitations. Sometimes it helps to describe what the category does not include, for instance:

  Security incidents include actions or events that cause, or create the potential for, a breach in system confidentiality. Password compromises are a good example. This category does not include inappropriate disclosures of system content by personnel who are authorized access to the data they divulge.
- Classifications equate items that are not of equal value, or that don't belong on the same level. In an outline, that's called faulty coordination.[4]

Use the technology.

Use updated technology to get the information to readers in the most usable form. There are a number of alternatives to fat binders, although most organizations would prefer to supplement, rather than replace, their hard copies.

For end users, consider providing the User Guide and other documents in the form of help files. These can either be Windows Help files, installed on the user's computer, or html Help files available on a web page. Either way, you can offer a table of contents, index, and search feature that help users find the information they need. Of course, if their computer is down, they won't be able to read Help files. But you can still offer the same material in a printed manual, and without the expense of starting over from scratch. Some help authoring software, such as eHelp[5], can readily export Help projects to print (Microsoft Word) format.

For System Administrators and other managers, consider providing reference material in electronic form, with a search engine that's really makes the information accessible. dtSearch[6] makes a product that can do Boolean searches, proximity searches, find stemming variations of words (e.g., find, finds, finding, etc.), use a built-in thesaurus, or let you build your own list of synonyms (such as your companies common abbreviations and acronyms); in short, a product that does much more than an ordinary word search. And it can either be purchased as a desktop software application, or prepackaged with a CD containing the references themselves.

A technological solution can be a cost-effective enhancement, especially when the bulk of the policy makes it difficult to handle in paper form.

[4] Irish, R. K., & Kwiatek, D. (1999). Engineering Writing Centre – handbook – outlines [WWW page]. URL http://www.ecf.toronto.edu/~writing/outline1.htm

[5] eHelp (1999). Demystifying help [White paper]. URL http://www.ehelp.com/RoboHelp/resources/whitepapers/

[6] dtSearch (2000). dtSearch Corp. corporate and product information [WWW page]. URL http://www.dtsearch.com/dtsoftware.html

The Result - Readable security policy documentation is more likely to be used.

When documentation is focused, concise and readable, it has a good chance of being accepted as a functional tool and thus achieving its purpose.

Sources Cited

AltaVista (n.d.). Art of technical documentation [WWW page]. URL http://shopping.altavista.com/product.sdc?n=24319&p=10333193

Department of Defense (2000). Department of Defense manual number 8510.1-M: Department of Defense information technology security certification and accreditation process (DITSCAP) application manual [downloadable file]. URL http://web7.whs.osd.mil/html/85101m.htm

dtSearch (2000). dtSearch Corp. corporate and product information [WWW page]. URL http://www.dtsearch.com/dtsoftware.html

eHelp (1999). Demystifying help [White paper]. URL http://www.ehelp.com/RoboHelp/resources/whitepapers/

Irish, R. K., & Kwiatek, D. (1999). Engineering Writing Centre – handbook – outlines [WWW page]. URL http://www.ecf.toronto.edu/~writing/outline1.htm

TechRepublic (n.d.). Search results – Tech Republic [WWW page]. URL http://www.techrepublic.com/search/result.jhtml?_DARGS=%2Fsearch%2Fquery.jhtml.5

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS