Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Technical Writing for IT Security Policies in Five Easy Steps

As management requires more policies, staff comfort levels drop. As policy writers include complex, confusing, and incomprehensible language, staff comfort levels continue to drop. Therefore, IT Security policy writers need a writing resource, not just a policy resource. This paper points new policy technical writers in the right direction and provides a solid foundation from which to start. Follow these five easy steps when writing IT Security policies. Your management and employees will thank you.

Copyright SANS Institute
Author Retains Full Rights

AD

Technical Writing for IT Security Policies in Five Easy Steps

J. Patrick Lindley
September 20, 2001

Introduction:

IT Security policies establish high-level rules to protect a company's technology resources and the data stored by those resources. These policies exist at many different levels in organizations. From enterprise-wide to local branch offices, policies inundate our daily work lives. Information Technology Security Awareness Training and Education (ITSATE) encourages policies in an effort to establish appropriate use of technology resources.

Management often tasks IT Security professionals with the creation of IT Security policies. Many good references exist to assist these professionals in policy writing. These resources describe what policies should contain in terms of purpose, scope, responsibility, etc. However, they don't address the need of providing specific guidelines for the novice technical writer. IT Security professional training frequently avoids the field of technical writing. Consequently, these professionals usually lack the skills necessary to create readable, concise and effective written communication.

As management requires more policies, staff comfort levels drop. As policy writers include complex, confusing, and incomprehensible language, staff comfort levels continue to drop. Therefore, IT Security policy writers need a writing resource, not just a policy resource. This paper points new policy technical writers in the right direction and provides a solid foundation from which to start. Follow these five easy steps when writing IT Security policies. Your management and employees will thank you.

Step One – *Who, What, Where, When, Why:*

IT Security policy writers craft effective policies by asking themselves five questions: *who*, *what*, *where*, *when*, and *why*. These questions provide a consistent framework for all technical writing. They especially apply to policy writing. By excluding this specific information, policy writers diminish the readability, effectiveness, and usefulness of their work. Journalists traditionally incorporate these five questions into their news stories every time. "By using them as probes, you'll look at your subject more closely, and as you do, you'll find pertinent things to say."[1] Policy writers increase reader comfort levels by following this advice. Readers require concise information because they are busy. Reading through paragraph after paragraph without finding pertinent information creates discomfort. This forces the reader to make assumptions about the written document. Prudent writers answer these questions within the first few paragraphs of their policies to increase reader comfort levels.

Policies, by definition are high-level documents and should not contain guidelines or procedures. Too often, policy writers include *how* things must be done, however "…good policies generally establish only what must be done and why it must be done, but not how to do it."[2]

[1] Guilford.
[2] Sato.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Readers choose to ignore what they don't understand. When security policies become so bloated with abstract information they become useless in a real world environment. Writers minimize policy bloat by sticking to these five fundamental questions. Well-written policies guarantee reader comfort.

Note that the questions "where" and "when" may be more appropriately included in procedures or guidelines instead of policies. The policy writer should research this requirement before writing begins.

Step Two – *Business Writing:*

Past business customs maintained that more is better. Now, however, less is better. "We write to communicate not to confuse or confound."[3] Writers often undermine their own good ideas by burying them in bureaucratic style and making the reader uncomfortable. Uncomfortable readers choose to ignore writing that makes them work harder. Policy writers contribute to reader comfort by following two simple grammar rules:

1: Juxtapose Subject and Verb. In a good sentence, the grammatical subject presents the topic of the sentence. In addition, the subject and the verb lend more credence in a sentence when they are positioned next to each other; referred to as "juxtaposed". The subject of the sentence is the actor or the "who". What the subject did is the verb or the action the actor took. Consider the following sentence:

The technology resources that make up the enterprise's IT assets constitute a sizable monetary investment that must be protected.

The word "resources" represents the subject and the word "constitute" represents the verb. By splitting the subject and verb, writers force the reader to wade through prepositional phrases, modifier words, and other common English language fluff before reaching the action of the sentence. Instead, juxtapose the subject and verb so the sentence reads:

The enterprise IT resources constitute a sizable monetary investment that must be protected.

This simple edit results in a more readable sentence by positioning the subject and verb next to each other. It also shortens it by six words. Shorter sentences contribute to reader comfort. "Many people write long, heavy, burdensome sentences that fatigue their readers."[4] Write concisely and stick to the facts. Readers appreciate the extra effort.

2: Write in the Active Voice. Passive voice implies a state of being. The verbs "to be," "to have," and "to do" are passive or static verbs. By following Business Writing Rule #1 above, writers easily craft active voice sentences. Identify the actor and you identify the sentence subject. Ask yourself "who does what?" in the sentence. Use this question as a test for every sentence in the

[3] Vanderwold, p. 9.
[4] Vanderwold, "Sentence Aerobics and Presentation".

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

policy. This helps determine if the "who" is "doing" the "what". Consider the following passive voice sentence:

The purpose of this policy is to establish acceptable and unacceptable email use.

The subject and verb are separated by the prepositional phrase "of this policy". The word "purpose" represents the subject and the word "is" represents the verb. The verb "is" describes a state of being (i.e. the purpose is). The word in subject position isn't the actor. Look in the prepositional phrase to find the actor. By rewriting the sentence in active voice, the sentence reads:

This policy establishes acceptable and unacceptable email use.

Notice that the active voice provides a clear actor performing an action (in this case the "policy establishes"). It also juxtaposed the subject "policy" and verb "establishes". This revision produced a much shorter sentence (see Business Writing Rule #1 above).

Active voice increases reader comfort by providing clear actors and actions as well as decreasing the length of sentences. "Experts warn you to eradicate the passive voice from your writing."[5] However, not every sentence lends itself to active voice. Some sentences, due to legal requirements or other necessities, must be worded in such a way as to include the passive voice. It is okay to have about 25% of a document in the passive voice. Try to stay at or below that percentage when writing policies. For example, this document contains only 2% passive voice (excluding the samples and sources pages).

Step Three – *Know Your Audience:*

California recently joined South Carolina, Delaware, Alaska, Connecticut, and other states to establish the High School Exit Examination (HSEE). It requires all prospective high school graduates to "demonstrate competency in the content standards for reading, writing, and mathematics, adopted by the State Board of Education (SBE)."[6] High school graduates must achieve the "SBE-adopted standards through grade 10"[7] including vocabulary, informational reading, literary reading, and writing strategies, applications, and conventions.

Many people read at or below the 10th grade level. Long sentences contribute to reader discomfort and increase reader confusion. Uncommon words encourage readers to either skip them or misunderstand them. Therefore, know your audience. "You 'adapt' your writing to meet the needs, interests, and background of the readers who will be reading your writing."[8]

Writing at the 10th grade level may seem like "dumbing down" the document. But when readers actually understand the written words in a policy, they more easily understand the policy. Readers who understand the policy are more likely to abide by it. Policy writers are the link to

[5] Nickerson.
[6] Standards and Assessment Division, California Department of Education. p. 6.
[7] Standards and Assessment Division, California Department of Education. p. 7.
[8] McMurrey.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

readers in communicating the contents of IT security policies. Producing policies with excessive technical jargon and "legalese" simply increases the document's length. Policy written at a level above the audience adds to reader discomfort.

Microsoft Word and other word processing software display statistical information about the content of the files created with them. In Microsoft Word, select the "Tools" menu and then the "Spelling and Grammar" menu item. Click on the "Options" button and put a checkmark in "Show Readability Statistics" in the Grammar section of the options window. Execute the spelling and/or grammar check from within Microsoft Word. When complete, the program displays statistics about the document including word counts, averages, and readability levels. Locate the "Flesch-Kincaid Grade Level" entry and note that value. That value denotes the grade level of the document. This paper's grade level is 10.7 (excluding the samples and sources page).

Step Four – *Brevity is Beauty:*

By focusing on Steps 1 through 3 above, policy writers include only the necessary information in their policies. They also reduce the overall length of their sentences. This in turn produces shorter policy documents. Reader comfort levels increase and management more readily supports the policy's final version.

If management prefers short, specific memos, why shouldn't policy readers expect short, specific policies? Policy writers increase reader comfort when creating one-page policies. Employees rarely read and possibly never use long-winded, many-paged policies. Industry professionals commonly refer to these long policies as 'shelfware'. "Part of the solution to the shelfware problem is to make the information as focused and readable as possible."[9] Policy writers accomplish this by researching policy requirements before writing.

Because IT Security policies cover a broad range of different topics (e.g. Internet Use, Workstation Software, E-mail, etc.), policy writers often put all of this information into one policy document producing a many-paged monstrosity. Policy writers improve reader comfort by separating each policy into a stand-alone document in and of itself. This technique assists policy writers by encouraging single-page policies. Readers focus their attention on the policy since the written information concentrates on a single subject.

[9] Desilets.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Step Five – *Put it all Together:*

My own policy writing experience taught me many things over the years. Not only did I learn about the four steps above but also found that readers prefer consistent style. Consistency produces reader comfort. I accomplish consistent style by creating a policy binder that incorporates the following three ideas:

1: The Font. Write all policies in the same business style typeface and font size. It is okay to include larger headers and smaller footnotes. However, be consistent with the policy body text. Pick one business style font and one size. Use it throughout all the policies not just the policy you are working on at that moment.

2: The Preamble. Create a 'preamble' page that includes items common to all policies. The 'preamble' contains information about *why* the policy exists, who enforces it, and what responsibilities staff members have. A 'preamble' page provides an excellent means of reducing common clutter in policies by moving repetitive sentences and paragraphs to a single location. Instead of writing the same information over and over for each policy, move it to the 'preamble' and state it once.

3: The Signature Sheet. Create one signature sheet for all the policies. It should include a list of all the policies. The signature sheet states that the staff member read and understood the policies. By signing the signature sheet, the reader confirms receipt of the policies and indicates comprehension of the contents. File signature sheets with the employee's other Human Resources information. Be sure to give a copy of it to the employee as well.

Management or Human Resources personnel increase reader comfort by putting all the single-page policies (including the 'preamble' and signature sheet) together into a policy binder. This creates a comprehensive policy set. This policy binder protects the organization's IT resources and helps promote ITSATE. Use your policy binder to instruct your staff and they'll use it when they need to look up policy compliance.

Considerations:

IT Security policies and policies in general contain common elements including but not limited to: ownership, monitoring, and accountability. Since these elements of policy contain information specific to each policy, include them in the policy to reinforce their importance. Readers learn that each element applies to all company resources.

Common business practice suggests that organizations update their policies every year. Review your policies yearly to keep them current. This practice contributes to reader comfort by incorporating newer, up-to-date, language in the policy. It further assists in reader comfort by ensuring that all technology resources are included in the policy. Policies that remain stagnant for many years become less effective over time. Readers forget the contents, management forgets the policy exists, and policy writers feel that they've wasted their time. Update all policies to keep them fresh.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Additionally, get a new signature every year. Readers sign the original policy and should therefore sign subsequent revisions. The Human Resources department commonly handles all signature documents. Provide ITSATE on a yearly basis and include the policy signing at that time. Be sure to include policy signing at new employee hire dates.

Good writers research business and industry requirements before writing policies. Industries (such as banking or government) often require specific legal information. Policy writers must take these requirements into consideration when writing policies. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) enacted on August 21, 1996 requires compliance for the healthcare industry. Therefore, prudent healthcare industry policy writers include language in their policies now that complies with this act. Waiting for final approval of each HIPAA requirement could mean re-writing your policies. Note that non-healthcare industry corporations may still be required to comply with HIPAA if they gather or hold healthcare information about its employees. HR departments commonly maintain information about what health plan its employees use. They might also keep copies of doctor's notes for excused absences. These items fall under HIPAA guidelines. The wise writer incorporates current and future legislation (like HIPAA) and other industry requirements into policies now rather than later.

Sample Policies:

I've included a sample 'preamble' and policy below. Feel free to use them as templates when writing your own policies.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Preamble

In compliance with the <industry rules>, the <corporate mandates>, and generally accepted industry best practices, the <company> provides for the security and privacy of the data stored on, redirected through, or processed by its technology resources. The <company> encourages the use of these technology resources, however they remain the property of the <company> and are offered on a privilege basis only.

Throughout this policy, the term "staff" identifies full- and part-time employees, contractors, consultants, temporaries, student assistants, volunteers, retired annuitants, vendors and other users including those affiliated with third parties who access <company> technology resources due to their job responsibilities. Management expects staff to comply with this and other applicable <company> policies, procedures, and local, state, federal, and international laws. ***Failure to abide by these conditions may result in forfeiture of the privilege to use technology resources, disciplinary action, and/or legal action.***

The IT Policy Review Team regularly modifies this and other IT security related policies to reflect changes in industry standards, legislation, technology and/or products, services, and processes at the <company>.

Privacy
The <company> reserves the right to monitor, duplicate, record and/or log all staff use of <company> technology resources with or without notice. This includes but is not limited to e-mail, Internet access, keystrokes, file access, logins, and/or changes to access levels. ***Staff shall have no expectation of privacy in the use of these technology resources.***

Liability
The <company> makes no warranties of any kind, whether expressed or implied for the services in this policy. In addition, the <company> is not responsible for any damages which staff may suffer or cause arising from or related to their use of any <company> technology resources. ***Staff must recognize that <company> technology resource usage is a privilege and that the policies implementing said usage are requirements that mandate adherence.***

Staff Responsibilities and Accountability
Effective information security requires staff involvement as it relates to their jobs. Staff is accountable for their actions and therefore they own any events occurring under their user identification code(s). It is staff's responsibility to abide by policies and procedures of all networks and systems with which they communicate. Access of personal or private Internet Service Providers while using <company> provided information technology resources or using non-<company> provided information technology resources to conduct <company> business does not indemnify any entity from the responsibilities, accountability and/or compliance with this or other <company> policies. Staff responsibilities include but are not limited to:

- Access and release only the data for which you have authorized privileges and a need to know (including misdirected e-mail)
- Abide by and be aware of all policies and laws (local, state, federal, and international) applicable to computer system use
- Report information security violations to the Information Security Officer or designee and cooperate fully with all investigations regarding the abuse or misuse of state owned information technology resources
- Protect assigned user IDs, passwords, and other access keys from disclosure
- Secure and maintain confidential printed information, magnetic media or electronic storage mechanisms in approved storage containers when not in use and dispose of these items in accordance with <company> policy
- Log off of systems (or initiate a password protected screensaver) before leaving a workstation unattended
- Use only <company> acquired and licensed software
- Attend periodic information security training provided by <company> IT Security Branch
- Follow all applicable procedures and policies

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Electronic Mail (E-Mail) Policy

The <company> electronic mail services (e-mail) policy provides staff with guidelines for permitted use of the <company> e-mail technology resource. The policy covers e-mail coming from or going to all <company> owned personal computers, servers, laptops, paging systems, cellular phones, and any other resource capable of sending or receiving e-mail.

Ownership
The <company> owns all e-mail systems, messages generated on or processed by e-mail systems (including backup copies), and the information they contain. Although staff members receive an individual password to access the e-mail systems, e-mail and e-mail resources remain the property of the <company>.

Monitoring
The <company> monitors, with or without notice, the content of e-mail for problem resolution, providing security, or investigative activities. Consistent with generally accepted business practices the <company> collects statistical data about its technology resources. <company> technical staff monitors the use of e-mail to ensure the ongoing availability and reliability of the systems.

Accountability
Staff may be subject to loss of e-mail privileges and/or disciplinary action if found using e-mail contrary to this policy. Staff must maintain the confidentiality of passwords and, regardless of the circumstances, ***never share or reveal them to anyone***. The Information Security Officer (ISO) must provide express written permission before sensitive information is forwarded to any party outside of the <company>. Staff should contact the ISO with questions regarding the appropriateness of information sent through e-mail.

Ethical Behavior and Responsible Use
The <company> provides e-mail systems to staff to facilitate business communications and assist in performing daily work activities.

Ethical and Acceptable
- Communications and information exchanges directly relating to the mission, charter, and work tasks of the <company>
- Announcements of laws, procedures, hearings, policies, services, or activities
- Notifying staff of <company> sanctioned employee events, such as the holiday party, bake sales, arts and craft fairs, retirement luncheons, and similar approved activities
- Respecting the legal protection provided by all applicable copyrights and licenses
- Practicing good housekeeping by deleting obsolete messages

Unethical and Unacceptable
- Violating ***any*** laws or <company> policies or regulations (e.g. those prohibiting sexual harassment, incompatible activities, or discrimination)
- Submit, publish, display, or transmit any information or data that contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, discriminatory, or illegal material
- Compromising the privacy of staff, customers, or data and/or using personal information maintained by the <company> for private interest or advantage
- Engaging in any activities for personal gain, performing personal business transactions, or other personal matters (e.g. sending sports pool or other gambling messages, jokes, poems, limericks, or chain letters)
- Intentionally propagating, developing, or executing malicious software in any form (e.g. viruses, worms, trojans, etc.)
- Viewing, intercepting, disclosing, or assisting in viewing, intercepting, or disclosing e-mail not addressed to you
- Distributing unsolicited advertising
- Accessing non-<company> e-mail systems (e.g. Hotmail, Yahoo!) using <company> owned resources

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Sources:

Desilets, Gary. "Shelfware: How to Avoid Writing Security Policy and Documentation That Doesn't Work." 20 April 2001. http://www.sans.org/infosecFAQ/policy/shelfware.htm (28 August 2001).

Guilford, Chuck. "Paradigm Online Writing Assistant: The Journalist's Questions." 1996 http://www.powa.org/whttowrt.htm#The%20Journalist's%20Questions (25 September 2001).

McMurrey, David A. "Online Technical Writing" Online Technical Writing: Audience Analysis. http://www.io.com/~hcexres/tcm1603/acchtml/aud.html (15 September 2001).

Nickerson, Doug. "Five Tips to Improve Your Technical Writing." 1999 http://techwriting.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fnovalearn.com%2Fwol%2FNickerson1b.htm (17 September 2001).

Sato, Miles M. "HIPAA Security Policy Development: A Collaborative Approach." 30 April 2001. http://www.sans.org/infosecFAQ/policy/HIPAA_policy.htm (28 August 2001).

Standards and Assessment Division, California Department of Education. "High School Exit Examination Updated Information for Districts, Schools, and Parents." 15 December 2000. http://www.cde.ca.gov/statetests/cahsee/CAHSEEInfoPkt12-00.pdf (15 September 2001).

Vanderwold, Linda B. "Sentence Aerobics Presentations and Workshops." http://www.vanwrite.com/sentence-aerobics.htm (12 September 2001).

Vanderwold, Linda B. Target Editing, Second Edition. Sacramento: VanWrite Publishers, 1999.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**