Global Information Assurance Certification Paper

An Information Security Policy Development Guide for Large Companies

Sorcha Canavan
GSEC Practical Version 1.4b – Option 1
November 18th, 2003

Abstract

Although the importance of information security for businesses is increasingly recognized, the complexity of issues involved means that the size and shape of information security policies may vary widely from company to company. This may depend on many factors, including the size of the company, the sensitivity of the business information they own and deal with in their marketplace, and the numbers and types of information and computing systems they use. For a large company, developing a single policy document that speaks to all types of users within the organization and addresses all the information security issues necessary may prove impossible. A more effective concept is to develop a suite of policy documents to cover all information security bases; these can be targeted for specific audiences, making a more efficient process for everyone.

This paper examines the elements that need to be considered when developing and maintaining information security policy and goes on to present a design for a suite of information security policy documents for a large company.

Determine Your Policy Requirements

Why Do You Need Security Policy?

A security policy should fulfil many purposes. It should:

- Protect people and information
- Set the rules for expected behaviour by users, system administrators, management, and security personnel
- Authorize security personnel to monitor, probe, and investigate
- Define and authorize the consequences of violation[1]

In addition, information security policies will help turn staff into participants in the company's efforts to secure its information assets, and the process of developing these policies will help to define a company's information assets[2]. Information security policy defines the organization's attitude to information, and announces internally and externally that information is an asset, the property of the organization, and is to be protected from unauthorized access, modification, disclosure, and destruction[3].

In short, security policy should be a useful tool for protecting the security of the Enterprise, something that all users can turn to in their day-to-day work, as a guide and information source. All too often however, security policies can end up

[1] SANS GSEC Security Essentials Training Materials, p.336.
[2] Danchev, pp.2-3.
[3] Peltier, p.4.

simply as "shelfware"[4], little read, used, or even known of by users and disconnected from the rest of company policy and security practice.

The key to ensuring that your company's security policy is useful and useable is to develop a suite of policy documents that match your audience and marry in with existing company policies.

Who Will Use Your Policies? – Count Your Audiences

Your audience is of course all your company employees, but this group can be divided into audience sub-categories, with the members of each sub-category likely to look for different things from information security policy. The main audiences groups are:

- Management
- Technical Custodians
- End-Users

All users will fall into at least one category (end-user) and some will fall into two or even all three.

The audience for the policy will determine what is included in each policy document. For example, you may not always want to include a description of *why* something is necessary in a policy - if your reader is a technical custodian and responsible for configuring the system this may not be necessary because they are likely to already know why that particular action needs to be carried out. Similarly, a manager is unlikely to be concerned with the technicalities of why something is done, but they may want the high-level overview or the governing principle behind the action. However, if your reader is an end-user, it may be helpful to incorporate a description of why a particular security control is necessary because this will not only aid their understanding, but will also make them more likely to comply with the policy.[5]

Allow for the fact that your readers will want to use the policies in a number of ways, possibly even in more than one way at one time. For example, when first reading a policy document, an end-user may be interested in reading the entire document to learn about everything that they need to do to help protect the security of the company. On another later occasion however, the user may reference the document to check the exact wording of a single policy statement on a particular topic.

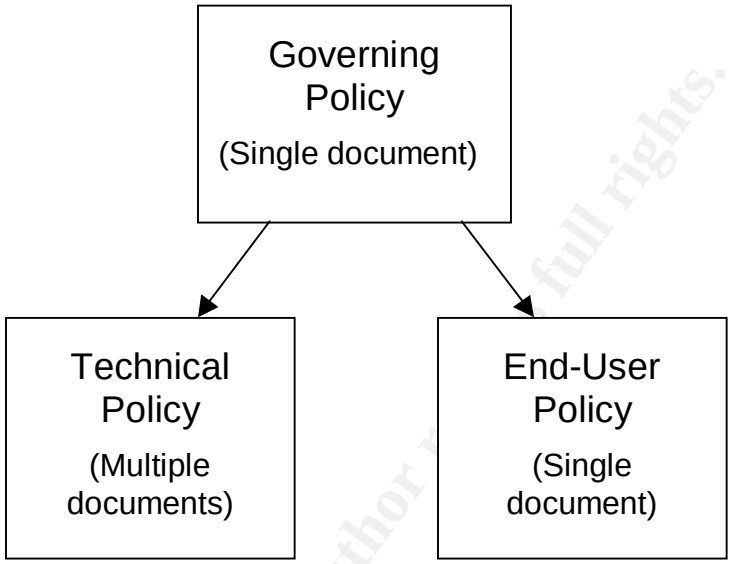
Given the variety of issues, readers, and uses for policy, how can we hope to address them in one document? The answer is that we can't. Companies must ensure that their information security policy documents are coherent with audience needs. In order to do this, they can use the methodology for

[4] Desilets, p.1.
[5] Russell, p.5.

developing a suite of information security policy documents described in this paper.

Policy Types – Governing, Technical, and End-User

The diagram below outlines a hierarchical policy structure that enables all policy audiences to be addressed efficiently:



As we have seen, in large companies there will be several audiences for your policy, and you will want to cover many different topics on different levels. For this reason, a suite of policy documents rather than a single policy document works better in a large corporate environment. The hierarchical structure of the suite of security policy documents reflects the hierarchical structure of roles in a large company. The proposed scheme provides for all levels of audience and for all topics by using three congruent policy types:

- Governing Policy
- Technical Policy
- End-User Policy

The policy development scheme outlined in this paper expands upon the three policy types (program policy, issue-specific policy, and system-specific policy) outlined in the SANS GSEC Security Essentials training[6]. The Governing Policy outlined in this paper is comparable to Program Policy, while program and issue-specific policy come under the heading of the Technical Policy as detailed here.

- **Governing Policy** - This should cover information security concepts at a high level, define these concepts, describe why they are important, and detail what your company's stand is on them. Governing policy will be read by managers and by technical custodians (particularly security

[6] SANS GSEC Security Essentials Training Materials, p.339.

technical custodians) and these groups will use the policy to gain a sense of the company's overall security policy philosophy. This can be used to inform their information security-related interaction with business units throughout the company.

Governing policy should be closely aligned with existing and future HR (human resources) and other company policies, particularly any that mention security-related issues such as email or computer use, etc. The Governing Policy document will be on the same level as these company-wide policies.

Governing Policy is supported by the Technical and User Policies which cover topics in more detail and add to these topics be dealing with them for every relevant technology. Covering some topics at the Governing Policy level may help obviate the need for a detailed technical policy on these issues. For example, stating the company governing password policy means that details of specific password controls can be covered for each operating system or application in the relevant technical policy, rather than requiring a technical policy on password controls for all systems. This may not be the case for a smaller company, where fewer systems/application are used and where a single technical password policy would be sufficient. For a larger company however, this provides a more efficient process for users to follow because they will have to reference fewer documents – simplifying this process raises the odds that users will comply with the policy, thereby improving security.

In terms of detail level, governing policy should address the "what" in terms of security policy.

- **Technical Policies** - Technical Policies will be used by technical custodians as they carry out their security responsibilities for the system they work with. They will be more detailed than the governing policy and will be system or issue specific, e.g., AS-400 or physical security.

  Technical policies will cover many of the same topics as governing policy, as well as some additional topics specific to the overall technical topic. They are the handbook for how an operating system or a network device should be secured. They describe what must be done, but not how to do it - this is reserved for procedural documents which are the next detail level down from technical and user policy.

  In terms of detail level, technical policy should address the "what"(in more detail), "who", "when", and "where" in terms of security policy.

- **User Policy** – This policy document should cover all the policy topics pertaining to information security that end-users should ever have to know about, comply with, and implement. Some of these policy statements may overlap with the technical policy, and all should be at the same level as technical policy. Grouping all end-user policy together means that users will only have to go to one place and read one document in order to learn

everything they need to do to ensure compliance with company security policy.

In terms of detail level, user policy should address the "what"(in more detail), "who", "when", and "where" in terms of security policy.

Additional Supporting Documents

- **Job Aids** – These are the documents that may be written where necessary in addition to and in support of any of the above types of policy documents, to aid readers in understanding what is meant in policy, through extended explanations. Beware however; if you find yourself getting requests for job aids for every policy document you write, your original documents may be too complex or hard to understand. Save you and your readers time by ensuring everything you write is clear, concise, and understandable in the first place.
- **Guidelines and Procedures** - Procedures and guidelines are an adjunct to policy, and they should be written at the next level down in terms of detail, describing *how* something should be done. They provide systematic practical information about how to implement the requirements set out in policy documents. These may be written by a variety of groups throughout the company and may or may not be referenced in the relevant policy, depending on requirements.

Policy Topics

When you begin to write security policy you will need to prioritize what topics need to be addressed first. A number of factors should be taken into account during this process. First, look at any areas containing information that you are legally obliged to protect. These areas will be defined (although not always clearly) in national, state, or local government laws. Secondly, look at information that may be used in critical decision-making by your organization or your customers. You may also be legally liable for compromises to the confidentiality or integrity of this information[7].

The remaining information should be prioritized according to business criticality and sensitivity, that is, how critical the information is to the continuation of your company's business processes and how much damage would result from unauthorized disclosure of the information. This will enable you to see which information is more sensitive. Your company's information security group may already have carried out a risk assessment, the results of which will help to determine which are priority policy topics.

Outline Topic List

When you have prioritized your information using the guidelines above, you can then begin to break it down by area into separate policy documents. Divide your

[7] www.itsc.state.md.us/info/InternetSecurity/BestPractices/SecPolicy.htm, pp.1-2.

topics by issue, system, and application. The categories and topics will vary by company but may include for example, many of those listed below:

Governing Policy

See the sample outline in Appendix 1 of this document for more detail on what Governing Policy should include.

Technical Policies

The number of technical policies required will depend on the number of operating systems, applications, and other technologies used by your company. Listed below are some categories that can be used to identify policy needs in each area. Each entry in a category represents a single technical policy document. This may seem like a large number of policies, but remember that the audience for these documents are technical people who work specifically with these technologies. Therefore, most technical staff will only have to read and know about the content of one or two technical policies. Information security employees will have to be familiar with a greater number of the documents.

Operating Systems

Windows
UNIX
Linux
Mac OS
OS400
MVS / OS390
Solaris
.NET

Enterprise Applications

Applications (a single document covering applications policy, and policy for web, vendor, and in-house applications)
Oracle
DB2
SQL Server
SAP
B2B

Network

Router
Remote Access
Extranet
Wireless

Exchange
Web Conferencing

Business Planning

Business Continuity
Disaster Recovery
Audit Trail
Data Classification

Security Devices

IDS (Network and Host-based)
Firewall

Peripheral Devices

Imaging/Output (including copier, printer, and fax devices)
Voice Communications
PDA

Cryptography

Encryption
Key Management

Physical Security

Physical Security

See the sample outline in Appendix 2 of this document for more detail on what a Technical Policy should look like.

User Policy

See the sample outline in Appendix 3 of this document for more detail on what an End-User Policy should look like.

Write Your Policy Documents

Policy Development Team

It is important to determine who is going to be involved in the actual development phase of policy at an early stage. The group who develops the policy should ideally also be the group who will own and enforce the policy in the long-term.

The policy development team will vary according to the policy document being developed, but the following is a list of individuals or groups who may be involved.

Primary Involvement:

- Information Security team – A team or part of a team from this group should be assigned the overall responsibility for developing the policy documents. Overall control may be given to one person with others in a supporting role. This team will guide each policy document through development and revision.
- Technical writer(s) – Your company or security department may already have a technical writer on staff who can assist in writing security policies. Even if they are not able to take primary responsibility for the information security policy project, an in-house technical writer can be a valuable resource to help with planning your policy project, determining an appropriate style and formatting structure for your documents, and editing and proof-reading your policy drafts.

Secondary Involvement:

The following groups may have input during the development of the policy in reviewing and/or approval roles.

- Technical personnel – In addition to staff on the security team, you may need to call upon the expertise of technical staff who have specific security and/or technical knowledge in the area about which you are writing. They will be familiar with the day-to-day use of the technology or system for which you are writing policy, and you can work with them to balance what is good security with what is feasible within your company.
- Legal counsel – Your legal department should review the policy documents once they are complete. They will be able to provide advice on current relevant legislation such as HIPAA and Sarbanes-Oxley, etc that requires certain types of information to be protected in specific ways, as well as on other legal issues.
- HR – The human resources department may need to review and/or approve your policy depending on how you have determined that your policy will relate to existing company policies. Where your policy touches on topics covered by existing HR policy, e.g., email usage, physical security, you must make sure that both sets of policy say the same thing.
- Audit – The internal audit department in your company are likely to be involved in monitoring company-wide compliance with the policy once it is in force. It is therefore useful if they are involved in the development and review processes for policy to ensure that it is enforceable in terms of their procedure's and current best practice.
- User groups – During revision of policy documents, it can be useful to work with users to determine how successful current policy is, and thereby determine how the policy may need to be changed (in a non-technical way) to make it more useable for your target audiences. Issues such as the style, layout, and wording of your policy documents may seem minor issues compared to their content, but remember that if your documents are off-putting or hard to understand, users may not read them fully or

may fail to understand them correctly, thereby risking needless security compromise.

Policy Development Lifecycle

Once you have determined who will be involved in writing the policy, you can begin the policy development process.

- **Senior management buy-in** – Developing a suite of policy documents will require a high level of commitment, not just from the primary developer/development team, but also from a number of other information security personnel in the company. In order to make sure that these resources are available to you for the time you need to get the information you need, management buy-in must be sought at the beginning of the policy project. Management must be made aware of both the importance and size of the task ahead so that they will not baulk at resource allocation in the later stages.
- **Determine a compliance grace period** - At the beginning of your overall policy development project, you should work with the internal audit group to determine how soon after policy publication they will audit based on the policy. By allowing a grace period for compliance, you are helping to ensure that the policies will be enforceable.
- **Determine resource involvement** – At this point you should identify who you will need to talk to about developing the policy in order to determine and agree on the content of the policy. See the Policy Development Team section for the categories of people who may need to be involved.

  You must give all team members an estimate of how much of their time they can expect to allocate to the project. Policy projects held up because subject-matter experts (SMEs) are busy can mean that the policy risks being out of date before it is finished. If necessary, get buy-in directly from line managers. In most cases, people will see the value of policy and will be happy to help you develop something that will help them in their jobs, but you need to make sure they are on board before going any further.
- **Review existing policy** – If your company has any existing policy, review it to determine if it can be used as part of the new suite of policy documents.
- **Determine research materials** – As well as talking to SMEs and other experts and drawing on your own knowledge of information security, you may need to do research for some policy topics. This is particularly the case for "new" technologies such as instant messaging, VPNs, or topics that your company has not previously had an official security policy on. In these cases, you will need to research industry best practices, and there are a number of sources you can use for this - I have listed some below:
  - Internet – As well as visiting information security websites, (e.g., www.securityfocus.com) use web search engines to find

information on security topics. However, stick to reliable sources and be aware that some of the information may not be current.

  - SANS – The papers in the SANS reading room provide excellent information on security topics which can be used as research material for policy topics.
  - Magazines, books, white papers.

- **Interview SMEs** - Before the interview itself, there are things you can do to ensure you get the best from your SMEs[8].
  - *Define your objectives* – know as much about the topic as you can, and determine what level of detail and information you require from the SME. The detail you require will depend on what type of policy document you are working. Let your SME(s) know what your objectives are so that they too can be prepared.
  - *Prepare for the meeting* – arrange a suitable meeting place or book a conference bridge. Compile a list of questions or an outline of topics you want to cover.
  - *Control the interview* – listen actively, ask open-ended questions and control the flow of the interview. Where SMEs disagree or go off on tangents, aim to bring them back to the focus of the discussion without getting into arguments about opinions. Take notes and write everything down. Ask questions if you are not clear on any points.
  - *Sum up and confirm* – sum up what you have understood from the interview and what your next steps are. Iterate anything that is expected from the SME before or in time for the next meeting. Thank them for their time.
  - *Post-interview review* – organize your materials, and review your notes while they are still fresh in your mind and on paper.
- **Write initial draft** - Determining the right pitch or level for the policy can make the difference between a feasible security policy and one that is merely shelfware. Make the policy too rigid and it will be unenforceable, but make it too weak and it will provide insufficient protection. Be aware that there may well be exceptions to some of the policy statements. In these cases, it is acceptable to leave the statements in the policy, but to refer the exceptions to the deviations process[9]. This ensures that the company policy is clearly stated and enforced according to risk assessment and best practices, while at the same time providing a

[8] Lambe, p.30.

[9] This process allows for requests for deviations from policy to be reviewed by a company's information security group. Applications are reviewed to determine if a deviation may be granted based on business needs, taking account of the risk to security. In many cases, deviations are temporary or on a small scale and do not present the security risk they would if allowed on a company-wide, permanent basis.

mechanism for dealing with occasional exceptions without weakening the policy.

Another consideration is to what extent the policy should reflect current practice versus preferred future. Writing a policy that reflects only precisely what is done today may be out-of-date even by the time it is published, while a policy that includes controls which cannot yet be feasibly implemented may be impossible to comply with for technical reasons.

The following style guidelines will help to ensure your policies are useable:

- Ensure you have a consistent style throughout. There is much debate about the passive voice versus the active voice; whichever you use, chose one and stick to it throughout to aid comprehension.
- Be clear and use concrete rather than abstract language, e.g., say "log files must be reviewed at a minimum annually" rather than "log files must be reviewed regularly". What is "regular" may differ from person to person and your policy must mean the same to everyone so that it can be followed consistently.
- Avoid using very negative statements such as "never". Using overly strong negatives sets up gradations of prohibition that are unhelpful when you want to present clear, useable policy that either allows or disallows actions, or presents exceptions clearly.
- Use simple, easy to understand language and pare it down to a minimum. All your readers must be able to understand your policy, and they shouldn't have to wade through reams of information to get to the point.
- Use "must" for "shall" and "will", where "must" is what you mean. You will therefore avoid inconsistencies in using "shall" and "will" and will not be mistaken for talking about the future.
- Don't include anything that isn't policy in the policy statements section of the document. Background information, for example, should go in a section of its own, either at the start of the document or in an appendix. You will weaken your policy statements by mixing them with informational statements. Similarly, procedural information should go in separate guidelines documents.
- Where you use bulleted lists in policy, ensure that all items in the list are grammatically similar. For example, if the list starts out as a list of nouns with modifiers, it shouldn't include any items that are verb phrases.

- **Review until complete** - Make a final check of your document to ensure that you have followed the style guides outlined above. In addition, carry out a final spelling and grammar check and have your document proof-

read by someone who wasn't involved in its development - this will help ensure that it is understandable and clear.

- **Review with additional stakeholders** – During this review phase the policy should be reviewed by any groups who have an interest in the policy. This includes any groups who will be expected to work with the policy, who may have knowledge that needs to be taken into account when developing with the policy, or who are able to help ensure that the policy is enforceable and effective. Such groups include the legal and internal audit departments. In addition, regional offices should be considered here, they will have to comply with the policy, but their requirements may be different from those of the central office and this should be considered in this review phase.
- **Gap analysis** – Before publishing policy, it is a good idea to determine which (if any) policy statements are not currently in force in your organization. Document any such gaps and determine which groups or individuals are responsible for closing them. Include these groups in the discussion and let them know that this policy will shortly be published and will have an impact on their working practice. This will ensure that people are prepared for the publication of the policy and no one will be deluged with enquiries upon publication. You will need to inform any groups identified during the gap analysis for each policy of the time-scale of the grace period for compliance so that they can plan towards future compliance.
- **Develop communication strategy** - Although the policy will be constantly available for company employees, you will initially need to make them aware of new or updated policy. Work with your communications or security awareness group to do this. Ensure that all appropriate management groups are informed, so that they can filter down information in their area.
- **Publish** – Policy documents should be published so that they available to all company employees, this usually means on a company intranet site, possibly the information security team's own intranet site. The documents should be easily accessible, and available for download, printing, and saving.
- **Activate communication strategy** - Email is probably the best way to inform employees about policy changes quickly and effectively, although you may also want to include information about policy in other forms of company communication and through your company's security awareness program.
- **Ensure policy is reflected in awareness strategies** - An effective security awareness strategy will ensure that all your audiences are aware of your security policy, where to find it and how to comply with it, as well as the consequences of non-compliance. Through a security awareness program, it should be possible to teach policy stakeholders about the

policy and their role in maintaining it, and this will help make the policy an integral part of their jobs[10].

- **Review and update** - Each policy document should be updated regularly. At a minimum, an annual review strikes a good balance, ensuring that policy does not become out of date due to changes in technology or implementation, but is more feasible than a review every six months which would require a very quick turnover of a large number of policies for a large company. There should also be a provision for ad hoc updates that are necessary when fundamental changes in technology or process render existing policies redundant.

  The review process should mirror the initial development process, but should be shorter, with the initial drafting phase telescoped into fewer meetings, or carried out over email. The time for review phases by groups outside the information security team can also be shortened by having all groups review the draft at one time.

  When reviewing existing policies, a number of factors should be taken into account in addition to those included during the initial development. The experience of working with the existing policy by users, systems administrators, or anyone else who has seen the policy in action is valuable here. These people should be interviewed on how they think the policy worked and what could be changed in the future. They will also provide valuable insights into changes in technology or industry best practices that may need to be reflected by a change in the policy. Any security violations, deviations, and relevant audit information should also be reviewed when reviewing existing policy[11]. This information will highlight any areas where the policy was difficult to enforce or where frequent deviations from policy were noted. It may be that elements of the policy are infeasible or need to be tweaked slightly to ensure that extra and unnecessary work on deviations is not created. This must as always be balanced with good security practice. Policy must primarily reflect what is necessary for good security. From a due diligence viewpoint, it is not acceptable to change good policy to inadequate policy just because there were a number of requests to deviate from that policy by certain groups within the company.

Policy Document Outline

In addition to the policy statements that will form the main body of your policy documents (see Appendices 1-3 for sample policy outlines), each policy should include the following sections:

- **Introduction** – This section should introduce the policy by name and locate it within the hierarchy of other existing information security and company policy documents.

[10] Barman, p.98.
[11] Barman, p.132.

- **Purpose** - State the main goals of the policy; this will explain the reason for the policy and will help readers understand how the policy should be used.
- **Scope** – The scope is a statement of the infrastructure and information systems to which the policy applies, and the people who are stakeholders in it. Stakeholders would typically include anyone who is a user of the information or systems covered by the policy.
- **Roles and responsibilities** – This is a statement of the structures through which the responsibilities for policy implementation are delegated throughout the company. Job roles may be specified in this section, e.g., Database Administrators (DBAs), Technical Custodians, Field Office employees, etc.
- **Updates and revisions** – This section defines who is responsible for making updates and revisions to the policy and how often these will take place. It may be useful to include a reference to the document as a "living document" which can be updated as determined by those responsible for updates and revisions. This will ensure that any ad hoc revisions are accounted for as well as scheduled updates. Information should also be included detailing where the policy will be published and how employees can access it.
- **Contact information** - Detail who should be contacted in connection with policy and how to report any suspected security violations - a group or mailbox rather than an individual is preferable here as these are less likely to change.
- **Definitions/Glossary** - Define any terms that may be unfamiliar to the reader. The necessity for this will depend on the audience, e.g., the readership of technical policy for Linux are likely to already be familiar with the Linux technical terms, therefore it will not be necessary to spell these out. The cryptography section of the user policy however may include terms with which readers are not familiar and these should be defined in footnotes or a glossary to aid comprehension.
- **Acronyms** - A separate section spelling out acronyms may be required where there are a large number or where the document is long or complex. For shorter documents, acronyms may instead be spelt out in the body of the document.

Conclusion

Policy is both the starting point and the touchstone for information security in any company. Policy provides evidence of the company's stance on security and provides a living tool for every employee to help build and maintain that level of security. It is therefore essential that security policy is accurate, comprehensive, and useable. In a large company it can be a

daunting task to produce policy that lives up to this standard. Assessing policy audiences, topics, and methods using the processes I have described in this paper will help to ensure that your policy documents are as efficient and useable as possible. In turn, this will help ensure that your efforts to raise the standard of security in your company are worthwhile.

References

Lindley, Patrick J. “Technical Writing for IT Security Policies in Five Easy Steps.” 20 Sept. 2001. URL: http://www.sans.org/rr/paper.php?id=492 (24 Sept. 2003)

Kok Kee, Chaiw. “Security Policy Roadmap – Process for Creating Security Policies.” 2 Oct. 2001. URL: http://www.sans.org/rr/paper.php?id=494 (24 Sept. 2003)

Long, Gerald P. “Security Policies in a Global Organization.” 25 Feb. 2002. URL: http://www.sans.org/rr/paper.php?id=501 (24 Sept. 2003)

Jarmon, David. “A Preparation Guide to Information Security Policies.” 12 Mar. 2002. URL: http://www.sans.org/rr/paper.php?id=503 (24 Sept. 2003)

Lambe, Jennifer L. Intercom, “Techniques for successful SME interviews.” Mar. 2000, pp.30-32

Danchev, Dancho. “Building and Implementing a Successful information Security Policy.” 2003. URL: http://www.windowsecurity.com/pages/security-policy.pdf (24 Sept. 2003)

Russell, Chelsa. “Security Awareness – Implementing an Effective Strategy.” 25 Oct. 2002. URL: http://www.sans.org/rr/paper.php?id=418 (24 Sept. 2003)

Harris, Shon, CISSP All in One Certification Exam Guide. New York: The McGraw-Hill Companies, 2002.

“Best Practices – Security Plans and Policies.” URL: www.itsc.state.md.us/info/InternetSecurity/BestPractices/SecPolicy.htm (24 Sept 2003)

Barman, Scott. Writing Information Security Policies. New York: Que, 2001.

Desilets, Gary. “Shelfware: How to Avoid Writing Security Policy and Documentation That Doesn’t Work.” 20 Apr. 2001.
URL: http://www.giac.org/practical/gsec/Gary_Desilets_GSEC.pdf (24 Sept. 2003)

Peltier, Thomas, R. “Information Security Fundamentals.” 2002.
URL: http://www.gocsi.com/ip.htm (29 Sept. 2003)

Appendix 1: Governing Policy Outline

The outline below gives the broad topic headings for a sample Governing Policy for an operating system or an application. The sections outlined in the Policy Document Outline section of this paper should also be included at the beginning of any governing policy.

Many of these topics will be relevant to the information security of all organizations, however some will vary according to the technology, systems, and applications used.

1. Authentication
2. Access Control
3. Authorization
4. Auditing
5. Cryptography
6. System and Network Controls
7. Business Continuity/Disaster Recovery
8. Compliance Measurement

Each section should detail what the company's stance is for each area in terms of the high-level results that should be achieved by following this policy and the high-level requirements that will enable this.

Appendix 2: Technical Policy Outline

The outline below gives the broad topic headings for a sample Technical Policy for an operating system or an application. The sections outlined in the Policy Document Outline section of this paper should also be included at the beginning of any technical policy.

Many of these topics will be relevant to the security of all organizations, however some will vary according to the technology, systems, and applications used.

1. Authentication
2. Authorization
3. Auditing
4. Network Services
5. Physical Security
6. Operating System
7. Business Continuity/Disaster Recovery
8. Compliance Measurement

Other technical policies such as physical security or audit trail policies will include some different types of information. The outline below gives the broad topic headings for a sample Physical Security Technical Policy.

1. Building Access

   (An example section with specific policy statements for inclusion under "Building Access" is detailed below)

   a. Emergency Exits

   - Emergency exits must be locked from the outside but not from the inside.
   - Emergency exits must be alarmed so that an alarm sounds when the exit is used.
   - Signs must be placed at each emergency exit to indicate that the exit is for emergency use only, and that an alarm will sound if the exit is used.
   - Exits and aisles must be unobstructed at all times.

2. Controlled Area Access
3. Equipment Protection
4. Housekeeping
5. Water Protection
6. Fire Protection
7. Air Conditioning and Electrical Power

Appendix 3: End-User Policy Outline

The outline below gives the broad topic headings for a sample User Policy. The sections outlined in the Policy Document Outline section of this paper should also be included at the beginning of any user policy.

Many of these topics will be relevant to the security of all organizations, however some will vary according to the technology, systems, and applications used.

1. User Access
2. User Identification and Accountability
3. Passwords
4. Software
5. System Configuration and Settings
6. Physical
7. Business Continuity Planning
8. Data Classification
9. Encryption
10. Remote Access
11. Wireless Devices/PDAs
12. Email
13. Instant Messaging
14. Web Conferencing
15. Voice Communications
16. Imaging/Output