Information Security Policy - A Development Guide for Large and Small Companies

Sorcha Diver

Information Security Policy –

A Development Guide for Large and Small Companies

Author	Version	Date
Sorcha Canavan	V1.0	11/18/03
Sorcha Diver (previously Canavan)	V2.0	07/12/06

1. Introduction

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 and the accompanying development process.

It should be noted that there is no single method for developing a security policy or policies. Many factors must be taken into account, including audience type and company business and size, all of which are discussed in this paper. One other factor is the maturity of the policy development process currently in place. A company which currently has no information security policy or only a very basic one may initially use a different strategy to a company which already has a substantial policy framework in place, but wants to tighten it up and start to use policy for more complex purposes such as to track compliance with legislation. When starting out it is a good idea to use a phased approach, starting with a basic policy framework, hitting the major policies that are needed and then subsequently developing a larger number of policies, revising those that are already in place and adding to this through the development of accompanying guidelines and job aids documents which will help support policy. The varying levels of maturity in policy development are discussed later in this paper in more detail.

2. Why Do You Need Security Policy?

2.1 Basic Purpose of 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]
- Define the company consensus baseline stance on security
- Help minimize risk
- Help track compliance with regulations and legislation

Information security policies provide a framework for best practice that can be followed by all employees. They help to ensure risk is minimized and that any security incidents are effectively responded to.

Information security policies will also 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].

2.2 Policy and Legislative Compliance

In addition to the purposes described above, security policies can be useful in ways that go beyond the immediate protection of assets and policing of behaviour. They can be useful compliance tools, showing what the company's stance is on best practice issues and that they have controls in place to comply with current and forthcoming legislation and regulations.

In today's corporate world it is essential for companies to be able to show compliance with current legislation and to be prepared for forthcoming legislation. Recent laws such as HIPAA (Health Insurance Accountability and Portability Act), GLB (Gramm-Leach-Bliley Act) and Sarbanes Oxley have had major implications for policy makers in the U.S. and farther a field. Policy can be used to help companies ensure they have the controls in place to work towards compliance by mapping policy statements to legislative requirements. In this way they can provide evidence that their baseline security controls are in line with regulations and legislation. This type of stance will also give companies an indication based on legal requirements of what they need to protect and to what

[1] SANS GSEC Security Essentials Training Materials, 2003. p.336.
[2] Danchev, pp.2-3.
[3] Peltier, p.4.

extent. This will help to ensure that they target security controls only where they are needed, a benefit from both a financial and personnel resourcing perspective.

2.3 Policies as Catalysts for Change

It is also possible to use policies to drive forward new company initiatives, with policy acting as the catalyst for future projects which move towards better security and general practices. For example, a policy stating that a certain type of encryption is required for sensitive information sent by email may (with prior consultation with the appropriate technical experts) help to promote the need to develop such a capacity in the future. The presence of this requirement in policy has made sure the impetus to develop the email encryption project has remained strong.

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

2.4 Policies Must be Workable

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 with existing company policies. Policies must be useable, workable and realistic. In order to achieve this it is essential to involve and get buy-in from major players in policy development and support (such as senior management, audit and legal) as well as from those people who will have to use the policies as part of the daily work (such as subject matter experts, system administrators and end users).

In order to achieve this, one important element is to communicate the importance and usefulness of policies to those who have to live by them. Often users seem to think that policy is something that is going to stand in the way of their daily work. An important element of policy development, and to ensure policies are put into practice and not rejected by the users, is to convey the message that policies are useful to users: to provide a framework within which they can work, a reference for best practice and to ensure users comply with legal requirements. Once users realise that policy is something that may actually help them as they do about their work, they are much more likely to be receptive to both helping you develop it and living up to it to ensure compliance. Similarly, once senior management realise that policy is a tool they can leverage to help ensure adherence to legislative requirements and to move forward much needed new initiatives, they are much more likely to be supportive of policy in terms of financial and resourcing support as well as becoming policy champions themselves.

[4] Desilets, p.1.

3. Who Will Use Your Policies? – Count Your Audiences

3.1 Audience Groups

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 – all levels
- Technical Staff – systems administrators, etc
- End Users

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

3.2 Audience and Policy Content

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 and to do this it is often necessary to use a number of different document types within a policy framework. Which type of document you use will be determined in large part by the audience for that document. For example, an overall Acceptable Use Policy will be in the form of a higher level document, while a document that describes how to configure the instant messaging system

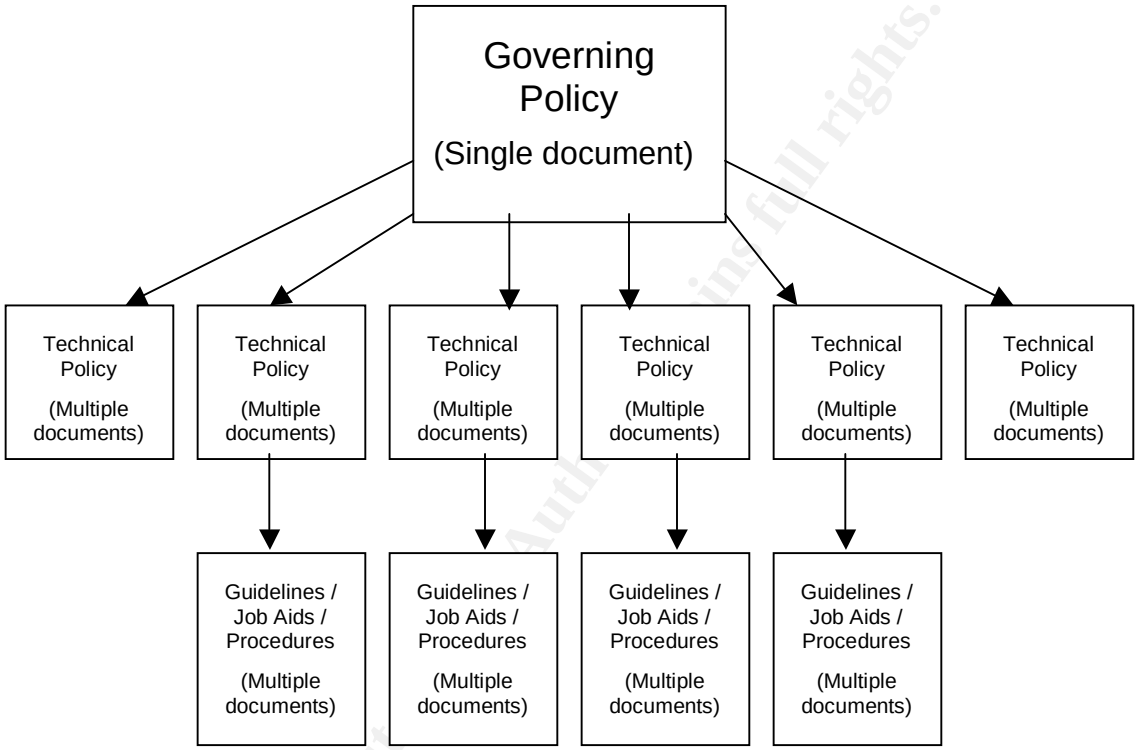
[5] Russell, p.5.

to ensure it complies with the Acceptable Use Policy may be in the form of a job aid or guidelines document. Manager and end users are likely to be interested the former, while administrative staff are more likely to use the latter.

4. Policy Types

4.1 Policy Hierarchy Overview

The diagram below outlines a hierarchical policy structure that enables all policy audiences to be addressed efficiently. This is a template for a policy hierarchy and can be customized to suit the requirements of any company:



The diagram above shows a hierarchy for a fairly mature, developed process, probably aligned to that possible in a large company where policy development has been underway for several years. For smaller companies or for those just starting to develop policy, it is possible to use this basic framework, but to initially have a smaller number of Technical Policies and possibly no guidelines or job aids early in the process. Rather than trying to develop a large hierarchy all at once, it is more realistic to develop a Governing Policy and a small number of Technical Policies initially, then increase the number of policies and supporting documents, as well as the complexity of the policies as you move forward.

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 two policy types supported by procedural documents:

- Governing Policy
- Technical Policy
- Job Aids / Guidelines

4.2 Governing Policy

Governing Policy 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 end users. By default it will also be read by technical custodians (particularly security technical custodians) because they are also end users. All 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 which 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 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's 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/applications are used and where a single technical password policy would therefore be sufficient. For a larger company however, the former method 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.

4.3 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 Governing Policy and will be system or issue specific, e.g., an AS-400 Technical Policy or a Technical Physical Security Policy.

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 Governing and Technical Policy.

In terms of detail level, Technical Policy should address the “what” (in more detail), “who”, “when”, and “where” in terms of security policy.

4.4 Job Aids / Guidelines

Procedural documents give step-by-step directions on the ‘how’ of carrying out the policy statements. For example, a guide to hardening a Windows server may be one or several supporting documents to a Technical Windows Policy. Procedures and guidelines are an adjunct to policy, and they should be written at the next level of granularity, 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.

Procedural documents may be written where necessary in addition to and in support of the other types of policy documents, to aid readers in understanding what is meant in policy through extended explanations. Not all policies will require supporting documents. 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.

The development of these supporting documents need not necessarily be undertaken by the policy development team who develop the Governing and Technical policies. It may be more efficient to have the individual business unit develop their own supporting documents as needed, both because of the availability of resources on the policy development team and because the technical staff in the business units are likely to have the most complete and up-to-date technical knowledge in the company, better enabling them to write such documents. The policy gives them the framework to follow (the “what”, “who”, “when”, and “where” in terms of security policy) and they simply need to follow these controls and sketch out the “how”.

Job aids and guidelines will also act as a backup facility if a staff member leaves, ensuring their knowledge isn’t lost and that policy requirements can still be carried out.

5. Policy Topics

5.1 Prioritizing 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[6].

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.

5.2 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 topics by issue, system, application, technology and general. You are then ready to determine which topics you need to reference in Governing Policy and which also need a separate Technical Policy of their own.

5.2.1 Governing Policy

Governing Policy should cover all aspects of security at a higher, broader level than the detail contained in the Technical Policies. All major, baseline security topics need to be covered. This is the place to state the company's baseline stance on these issues.

When first developing a Governing Policy where none previously existed the main concern may be to cover the main topics, while subsequent revisions may incorporate more company-specific topics as feedback is received and the policy development team has more familiarity with what issues need to be addressed.

The list of what can be included here is therefore virtually endless, but a starting point can be the sample Governing Policy outline in Appendix 1.

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

5.2.2 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 is by no means an exhaustive list and while the list for any given company will be dictated by the technologies in use by the company, some policies will be almost universal and most companies will need to consider developing a policy for these areas. 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.

Another way of structuring technical information security policies is to group by security topic, e.g., one policy on authorization, another on authentication, another on securing sensitive information, etc. There are times when this works well (physical security, privacy) and times when it isn't so successful (authentication, authorization), particularly for companies whose policy development model hasn't reached full maturity. The company's baseline stance on authentication fits comfortably into the Governing Policy for example, but when it comes to the detail on authentication (differences between platforms, etc) this is best tackled in the Technical Policy for as many technologies as need it rather than in a single authentication policy.

The reason for this is clear if you think again about how your users are likely to use the policy. Most users who need more detail than is contained in the Governing Policy will be searching for policy statements on a given technology ("I need to secure this Windows server, can you point me to the correct policy, please") rather than on a given topic. Therefore they would not welcome having to searching through policies on authentication, authorization and auditing to find out how to configure a given operating system or application.

The list below is a sample list of some of the policies a company might expect to develop[7]. Note however that the universal list is virtually endless and therefore each company's list will be different. Depending on how your company is set up, you may also group these policies differently, for example it may make sense to include your policy statement on VPN in your Remote Access Technical Policy in some cases. Another company might decide to have a single Technical Policy dealing with all peripheral devices while a larger company which uses many types of these devices might decide to have several policies dealing with individual devices types.

[7] This list is based on my own experience with the addition of suggested policies from Guel, p.11.

Operating Systems

Windows
UNIX
Linux
Mac OS
OS400
zOS
Solaris

Applications

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

Network

Router / Switch
Remote Access / VPN
Extranet
Wireless
Exchange
Web Conferencing

Business Planning / Administration

Acceptable Use
Acquisition / Procurement Assessment
Business Continuity
Disaster Recovery
Email Usage
Audit
Customer Authentication
Privacy
Third-Party / Service Provider
Patching

Risk Assessment
Information Sensitivity / Privacy
Information Management (including retention policies)
Password
Access Reverification
Data Classification

Security Devices
IDS (Network and Host-based)
Firewall
Anti-Virus

Peripheral Devices
Copiers, printers, and fax devices)
Voice Communications (including VOIP)
PDAs and other portable devices such as USB keys, flash drives
CDs/DVDs

Cryptography
Encryption
Key Management

Physical Security
Physical Security
Lab Security

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

5.2.3 Job Aids / Guidelines

The possible list of procedural documents a company might need is perhaps even more varied than the technical policy list. As these may be developed based on policy by individual business unit's rather than by the policy development team, in a large company you may not even know how many are out there. In other circumstances the policy development team will assist with the development of these documents.

Some example procedural documents are:

- Coding Guidelines: These will be developed for each programming language or coding environment used in a company and can be as detailed as necessary. They will include practical examples of

secure coding methods as well as broader secure coding policy statements. Input from the developers themselves is essential here.

- Business Recovery Plan Guidelines: These will describe the process for developing and maintaining a business recovery plan, including details such as roles and responsibilities of who owns the plan, who has the ability to update it, etc. In addition the guidelines could list the required plan elements and how often the plan should be tested.

6. Policy Development Process

6.1 Development Approach

6.1.1 Development Process Maturity

The major consideration behind any company's policy development process will be the level of process maturity. It is important that companies (especially larger ones) don't aim too high initially and try to develop a comprehensive and complex policy program straight away. This isn't likely to be successful for a number of reasons including lack of management buy-in, unprepared company culture and resources and other requirements not in place. In this situation it is advisable to start off small, perhaps developing checklist–style policies initially and only a skeleton policy framework with essential policies developed first.

As the process grows in maturity, companies will be able to develop the full range of policies with more detail included in each as well as accompanying procedural documentation as needed. Education, awareness and communication processes will also grow in maturity to cope with promoting an ever-growing range of policies. This should coincide with the growing corporate strength of the policies themselves. The corporate culture will start to appreciate that the policies must be followed and may actually start to use them to push through much needed changes throughout the company.

6.1.2 Top-Down Versus Bottom-Up

There are many starting points for developing policy. New or forthcoming legislation can often be a powerful impetus to develop policy, as can recent security incidents or enthusiastic administrators recently returned from the latest training course. All these provide great inputs to policy but the key is to be balanced. Relying solely on the 'top-down' approach of using only legislation, regulations and best practice to write your policy will leave you with unrealistic, artificial policy that won't be workable in the real world. Similarly, relying only on a 'bottom-up' method based only on system administrator knowledge can result in policy that is too specific to a given environment (perhaps just one part of a large company), possibly based too much on local current practice or on the latest training suggestions, making it too unrealistic. The best policy will come from a combination of these approaches, both top-down and bottom-up. In order to achieve this it is something that must be considered from the outset and must be reflected in the diversity of areas involved in policy development and the types of review policy undergoes.

This balanced approach is likely to result in a more mature policy development process. It can work for both small companies (where there is little space between top and bottom) and big companies where the

breadth of knowledge is needed to ensure a realistic and workable resulting policy.

6.1.3 Current Practice Versus Preferred Future

Policy development must also take into account 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 and may therefore be ignored as unrealistic and unworkable. It is important that this is discussed at an early stage as if it is not discussed and the policy develops too far towards the unworkable, preferred future model, this may only then show up at the policy gap identification stage, when a lot of time and effort will then have been wasted developing something which is of little value. The best policy strikes a balance between current practice and preferred future and this is what the policy development team should aim for.

6.1.4 Consider All Threat Types

Finally when considering what should be included in an initial draft, make sure to consider all the types of threats your company faces. While those from malicious external attackers in the form of viruses and worms attract much media attention and accordingly deserve to be considered when writing policy, other considerations that are at least as important include natural disasters, disgruntled current and former employees and ignorance leading to accidental security exposures. Policies should consist of controls to combat all these threat types.

7. 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; this is likely to be the information security department.

The overall composition of 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.

7.1 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 and should subsequently be available to answer questions and consult on the policy.

- *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.

7.2 Secondary Involvement

The following groups may (and in some cases, should) 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. The Legal department should also have input into the policy development process in terms of

letting the policy development team know about forthcoming legislative requirements and helping to decipher these for the team.

- *Human Resources* – 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 and Compliance* – 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 procedures and current best practice. If there are other compliance groups additional to the main internal audit department, these groups should also be consulting as needed.

- *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 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 needlessly risking security compromise.

8. Policy Development Lifecycle

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

8.1 Senior Management Buy-in

Developing a suite of policy documents will require a high level of commitment, not just from the primary developer and 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.

Senior management also supports the policy development and maintenance process by championing the resulting policies throughout the company and putting their weight behind them so that the policy is seen to have "teeth". Further, they should be prepared to support projects that result from policy to ensure compliance. These two types of support are essential to the ongoing viability of the policy program.

8.2 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. This grace period will ensure those users who have to live by the policies have enough time to review them and implement any project, processes or internal communications necessary to make sure they are in compliance. Depending on the size of the company, the grace period can be anything from a few months to around one year.

8.3 Determine Resource Involvement

At this point you should identify who you will need to talk to 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.

8.4 Review Existing Policy

If your company has any existing security policy, review it to determine if it can be used as part of the new suite of policy documents. Collect all related procedures and guidelines as well as any high level policy documents. These can all be used to get an idea of current company stance on a given issue or technology, or simply to show that a certain technology is secured differently in different areas of the company. This is something that will need to be reflected in the new policy document. Even existing guidelines or job aids can become the starting point for a policy document on the same topic.

8.5 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, smartphones, 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.
- Journals, books, white papers – Again, by aware of how up to date these sources are. In the fast-moving infosec world, books may soon get out of date; journals may be a better source in these cases.

8.6 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

[8] Lambe, p.30.

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.

8.7 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 mechanism for dealing with occasional exceptions without weakening the policy.

Even if you don't have fully formed policy statements at this point, it is a good idea to get something down on paper before your first review meeting with the rest of the project team. Even a list of topic headings and questions is easier to work from than a blank page.

8.8 Style Considerations

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

- Consult your corporate style guide. If one exists, this will be an easy way to ensure all your policies have the same look and feel and will also help them to be more quickly accepted as corporate documents. If you don't have a style guide, consider developing one to ensure consistency throughout your policies. This will also make them easier to update and review.
- 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 considered "regular" will differ from person to person and your policy must mean the same to everyone so that it can be followed consistently.

[9] This process allows for requests for deviations from policy to be reviewed by a company's information security group. Deviation 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.

- 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. In the following example, the first policy statement weakens the second because of the statement that one action “must never” be done while the other is prohibited with the, by comparison softer, “must not”:
  - “Passwords must never be shared.
  - Passwords must not be written down.”
- 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.
- Don’t include the names of individuals in policy. People are likely to change job rile more frequently than you will change the policy. Instead use job role names or department names, e.g., “the DBA team manager”.

8.9 Review Cycles

Review the draft with the project team as often as you need to ensure it is complete and correct and they are happy with it. Then 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.

8.10 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.

8.11 Policy Gap Identification Process

Before publishing policy, it is a good idea to determine which (if any) policy statements are not currently in force in your organization. These are known as gaps. 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 identification process for each policy of the time-scale of the grace period for compliance so that they can plan towards future compliance.

If you've pitched your policy correctly, you shouldn't find a very large number of gaps. Finding that every statement in the policy is actually a gap indicates that it is pitched too far towards a preferred future state and you may need to rethink some or all of the content.

Once you have identified any gaps, it is a good idea to keep a record of the gaps for each policy somewhere (e.g., in a database or even simply a spreadsheet). This should be checked regularly to see if any of the gaps are now closed or if any have passed the compliance grace period and need to be revisited. This record will also be a useful resource when you come to revise the policy in the future. Maintenance of this record may be the responsibility of the policy development team, the wider information security team or other areas such as Internal Audit. Make it clear where this responsibility lies at the outset.

8.12 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.

It stands to reason that if policy is not read it will not be adhered to, so don't underestimate the importance of successfully communicating policies to the various audience groups. Depending on the size of the company and the maturity of the policy development process this will be more or less complex. Smaller companies have an easier job in one way in that it is logistically easier for them to reach all employees and let them know what they should be reading and following. It is also likely that smaller companies will have fewer policies for their employees to read since they will usually have fewer technologies in use. However, even getting employees to read the Governing Policy can be a challenge, especially existing employees when the policy changes. Here are a few suggestions for how to tackle this:

- *Make it a contractual requirement:* This is usually reserved for HR-owned policies which employees must adhere to as part of their employment contract. However, because of the growing importance of information security in the corporate world, there is a growing argument for having

employees sign up to information security policies as well as general HR policies.

- *Make policy part of required training:* Incorporating information security policies into a training course (or courses) and making it a requirement for employees to complete these courses annually is another way to ensure policies get read and hopefully adhered to following course completion.
- *Use a subscription-based communication method:* One more advanced method of getting policies right under the noses of the employees who need to read them, and ensuring that the employees actually want to read them rather than considering them a nuisance, is to offer a subscription-based service where employees sign up to receive whichever policies are most appropriate for them. This 'sign up for security' method is something that could be activated when employees join the company, but could include a facility for employees to update their subscription options whenever they want to, for example if they move departments or change job role. While for larger firms this solution would require building a subscription service and maintaining it, smaller firms may be able to use a manual system that could provide this sort of service fairly easily.

8.13 Publish

Policy documents should be published so that they are available to all company employees. This usually means putting them 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.

Determining the most appropriate policy delivery method is a particular issue for large companies or those with large numbers of policies that don't apply to all employees. As already discussed in the communication strategy section, a tailored system of policy delivery would mean that an employee would receive directly only those policies they needed to comply with to do their job. This would make it much more likely that the employee will read and comply with the policy versus a conventional system where they have to seek out the relevant policies from a larger policy bucket.

8.14 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 policies, know where to find them and how to comply with them, 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. This will help make the policy an integral part of their jobs[10].

[10] Barman, p.98.

It is through using communication and education programs that you will be better able to foster a positive attitude in your company towards information security. There is evidence to show that users of the information security systems would be more willing to adhere to better security practices if they were knowledgeable (i.e., better trained and better informed) about what good practice actually involved[11].

A major part of ensuring policies have value is to ensure the employees who are supposed to follow them are aware of them and perhaps even more importantly, are aware of the value of adhering to them. This can be a big cultural shift in any organization. People often say things like: "but we've always done it that way" or "it doesn't matter if those SSNs go missing because we have stored them elsewhere". What security awareness campaigns must reflect is that the world has changed and it isn't about protecting the information just well enough so that it can be used for whatever purpose the company needs it for. There are now laws requiring companies to protect information at all times and to inform customers where security breaches occur. Therefore it isn't enough just to do things as they have always been done or not to keep records of what customer information is stored where. This may have been enough previously, but what your security awareness campaigns need to reflect is that things have changed and the front line in ensuring information is protected are the employees. Once employees realize that even relatively small security breaches can have potentially devastating (and job jeopardizing) consequences, they are much more likely to be willing to act as your first line of defense and to pick up your policies and start adhering to them. Awareness, education and policy go hand in hand, each strengthening the other.

8.15 Regularly 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, or parts of them, 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 the same 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

[11] JISC, p.3.

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[12]. 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.

[12] Barman, p.132.

9. Policy Document Outline

In addition to the policy statements that will form the main body of your policy documents (see Appendices 1-2 for sample policy outlines), each policy should include the following sections.

9.1 Introduction

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

9.2 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. Legal and compliance issues should also be mentioned in here. Include statements on any specific legislation the policy is designed to adhere to.

9.3 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.

9.4 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.

9.5 Sanctions and Violations

This section details to what extent breaking policy is considered a violation (e.g., it is HR-related and therefore related to an employee's contract, or is it an information security department matter?) This section should also detail how violations should be reported, who to and what actions should be taken in the event of a violation. It should also include information on what sanctions will be carried out resulting from a violation (for example, verbal or written warnings, etc).

9.6 Revisions and Updating Schedule

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.

9.7 Contact information

Detail who should be contacted in connection with policy. A group or mailbox rather than an individual is preferable here as these are less likely to change.

9.8 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 a 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.

9.9 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.

10. Troubleshooting

This section details some of the things that go wrong during policy development and some ideas to remedy these problems.

10.1 Policies Lack Weight

It is a big concern when policies that have taken time and effort to develop are not taken seriously. This is common when starting to develop information security policies and for those whose development process isn't yet mature. Don't worry too much at these early stages. Weight is likely to come with time and increasing numbers of policies, backed up and promoted by a combination of management backing and a good awareness/communication campaign. With this will come a realisation on the part of the enterprise (and particularly those bodies involved in compliance and governance) that policy can be used to leverage change and a move towards best practice and compliance.

10.2 Lack of Reviewing Feedback

Lack of feedback following reviews can also be a fairly common complaint from the policy development team. This is fine if the reviewers have read the policy and simply don't have any feedback; the problem arises when they have skimmed over the document without reading it closely or taking in the implication of its content. In these cases problems may only be noticed at a much later stage or, even worse, after publication. This can serve to weaken the policy and even discredit the policy development process as a whole.

One solution is to review each document in detail at a meeting (or meetings) with each group of reviewer. The development team representative can read through each policy statement and seek feedback on each one. This will help make sure the reviewers have both read and thought about the policy in detail.

Sometimes reviewers may not be sure what is required of them and this may result in a low level of feedback. To avoid this, inform all your reviewers about the process and what is expected of them (e.g., you are looking for feedback on the technical content of the policy rather than on typos and grammar errors).

Another possible reason for this is simply not giving the reviewers enough time to review. Be aware of their workload and agree a realistic timescale in advance. If you are dealing with review groups regularly for more than one policy, agree a regular timescale and stick to this.

10.3 Resources Shortage

This is frequently caused by two things: lack of management support and genuine resource shortages due to high workloads and cost cuttings exercises.

If you really can't get access to those people you need to to write the policy, consider putting it on hold until the resources are available. Try management your plan and point out that the company will be without the policy until resources can be found. This may change their mind or they may decide that other things take priority.

10.4 Reviews are Slow and Cumbersome

Sometime reviewing policy can seem to go for a long time. This can be because the project team size is too large. The optimum size for the core team is around 3 people. 2-4 is fine but any more than 4 and you start to have to take a lot longer to air everyone's views on each policy statement. If there are other people who are keen to be involved, keep the project team small but have the additional people review the policy as external stakeholder in a review period of their own. This way not everyone has to be consulted every step of the way but everyone still has an input.

Another reason for slow reviews is that often no one wants to take responsibility for making a decision. This is particularly the case on more contentious issues such as whether to allow instant messaging for all employees or what kind of mobile devices are allowed to be used. Reviews can often get stuck if no one wants to make the final decision. As always, take account of all opinions but try not to let policy get stuck on this. Maybe make a softer policy statement in the interests of getting something published. You might find in 6 months things have changed and a decision can be reflected in a more strongly-worded updated policy.

10.5 Legislation Compliance Queries

How do we know if we are complying with legislation? This is a commonly asked question in relation to policy. To ensure compliance, it is important to use your Legal and Compliance teams. Get their input on what is required and tie your policy statements to specify legal or regulatory requirements.

For larger companies, consider investing in a policy management system which will help you to track where your policies correlate with legislation and best practice.

10.6 Policy is Quickly Out of Date

If your users are complaining that policy is out of date when it is published, take this seriously. It is another issue that can quickly discredit your policy development program.

Reason for this include your review process being too slow (see section 7.4) or that policy is too focused on current practice and future changes aren't considered during the development stages. Make sure to consult your reviewers on where they think security is heading in the future for a given technology or

application. This will ensure this is reflected in policy as well as what happens today.

10.7 Policy is Unclear

If people can't understand or interpret your policies, they are unlikely to comply with them. Indeed, policies shouldn't be open to interpretation; they should be clear and concise, with each statement having only one possible meaning. To ensure this is the case, use a style guide and the services of a technical writer or an editor for each policy. Make sure you have a proper final review process in place where your policy is proof-read before being published. This should get rid of any last-minute typos or issues that will prevent comprehension.

10.8 People get Upset by the New Policy

People don't like change. Especially when they have been doing something one way for a long time, they don't like to told that there are now new rules that say they have to do it differently – even if those new rules will make their lives easier in other ways once they've got over the short term pain of making the changes. These are the simple reasons why there is often resistance to new and revised policies. Some of the industry's most experienced security experts have encountered this phenomenon[13] and it is something that you can expect to contend with throughout the policy development process.

Users will often have well-founded reasons for being concerned. They don't want to be bound by tight controls that make their job more difficult and management are concerned by possible increased costs associated with putting the policy into practice[14]. The best you can hope for here is to draw their attention to the benefits of developing the policy and point out that you need their help to do it properly and so that their fears aren't realized. Users and system support staff will often be concerned that the policy development team is going to force policy upon them without any comeback and this can make them resistance to participating in the development process. Be sure to fully explain your process to them at the start and make it clear that you need their input. Be firm, this policy is getting written, but you want to make sure it is workable and you want their help to do this. You anticipate that once it is in place it will actually help them in their job role because it will give them a clear template for which controls they have to adhere to. See section 2.4 for more detail on this issue.

Lastly, persevere. Initial reluctance can often give way to beneficial input and good support later on.

[13] Guel, p.5.
[14] ibid.

11. 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. 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

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

Danchev, Dancho. "Building and Implementing a Successful information Security Policy." 2003. URL: http://www.windowsecurity.com/pages/security-policy.pdf (10 July 2006)

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 (10 July 2006)

Guel, Michele D. "A Short Primer for Developing Security Policies." 2001.
URL: http://www.sans.org/resources/policies/Policy_Primer.pdf (12 July 2006)

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

Jarmon, David. "A Preparation Guide to Information Security Policies." 12 Mar. 2002. URL: http://www.sans.org/rr/paper.php?id=503 (10 July 2006)

JISC, "Developing an Information Security Policy", 1 May 2001. URL: http://www.jisc.ac.uk/index.cfm?name=pub_smbp_infosec (10 July 2006)

Kok Kee, Chaiw. "Security Policy Roadmap – Process for Creating Security Policies." 2 Oct. 2001. URL: http://www.sans.org/rr/paper.php?id=494 (10 July 2006)

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

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 (10 July 2006)

Long, Gerald P. "Security Policies in a Global Organization." 25 Feb. 2002. URL: http://www.sans.org/rr/paper.php?id=501 (10 July 2006)

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

Russell, Chelsa. “Security Awareness – Implementing an Effective Strategy.” 25 Oct. 2002. URL: http://www.sans.org/rr/paper.php?id=418 (10 July 2006)

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

Appendix 1: Governing Policy Outline

The outline below gives the broad topic headings for a sample Governing Policy. 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. Responsibilities – Information Security and Audit Departments
2. Email and Internet Use
3. Ethics and Appropriate Use
4. Personnel / Administration
5. User Identification and Accountability
6. Managing Users Accounts
7. Authentication

   This section might include statement like:

   - *User IDs and passwords must not be shared.*
   - *Passwords must not be written down.*
8. Access Control
9. Authorization

   This section might include statements like:

   - *Authorization must only be granted to access company information and systems to the level required for a user's job role.*
   - *Authorization to access information and systems must be re-verified at a minimum annually.*
10. Auditing
11. Physical
12. Hardware
13. Software
14. Incident Response
15. Intrusion Detection
16. Cryptography
17. Data Classification

18. System and Network Controls

    Including software settings and system configuration and settings and patching

19. Business Continuity / Disaster Recovery
20. Compliance Measurement
21. Change Management
22. Information Handling

    Including printing, copying, faxing, mailing, emailing, etc

23. Information Backup
24. Remote Access
25. Third Party / Service Provider Management
26. Network Connections

    Including internal and external and wireless

27. Instant Messaging
28. Web Conferencing
29. Voice Communications
30. Application Development

Each section should detail what the company's stance is for each area in terms of the high-level requirements.

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. The list below can be used to generate idea for policy statements in each area, but it isn't necessary to use all the categories in each case, sometimes they just won't apply.

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

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

1. General Requirements
2. Authorization - 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.

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