Security Policy overview

This chapter includes:

The Role of Policy and Procedures in Information Systems Defense

Interpreting Policy as an Auditor

Identifying Preventive, Detective and Corrective Controls

Security Policy Development

Introduction

Policy protects people and information. Without policy the organization is like a ship without a rudder. Most critically, policy is the primary guideline against which an audit is conducted. If the policy and procedures are lacking, the audit will also lack rigor.

There are numerous examples that have been taken from the SANS security Policy project (http://www.sans.org/resources/policies/) throughout this chapter. These excerpts have been used with permission from SANS.

SMART methodology. This is:

- Specific detail each component
- Measurable ensure that your record sizes, times and other relevant material
- Achievable ensure that you have the resources to achieve your objectives
- Realistic report the facts, don't speculate
- Time-based both work to time constraints and deadlines and ensure that you recorded all the events as they have occurred on the system.

The Role of Policy and Procedures in Information Systems Defense

Policy is what defines and authorizes the control framework that an organization will deploy. The vast majority of organizations fail to affect a useful policy framework for a number of reasons. Following the SMART principle is the best way to ensure that the policy framework can achieve the goals of the organization.

SMART

The concept of SMART is covered in a number of chapters in this book. In this section, the relationship of SMART to audit is explained. When assessing policy or procedure documents, it is important to ensure that the policy or procedure conforms to all five components of the SMART principles.

The technique for applying the concept of in depth defense to information systems security within an organization includes the following stages (see figure 6.1):

1. Determine assets and security objectives or the organization,
2. Specify the organization and overall architecture and stance,
3. Develop the policy, procedures and standards,
4. Implement and test the control systems, and
5. Continuously and periodically evaluate the controls that have been implemented with an eye to improvement.

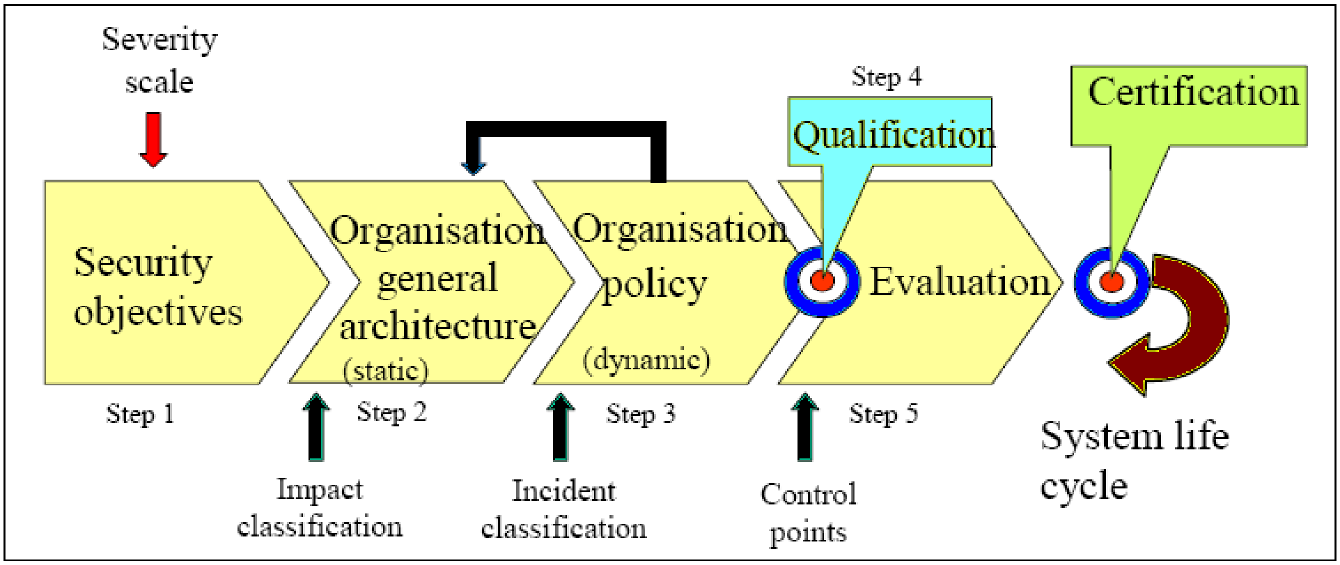


Figure 6.1 The stages in developing a secure organization

As can be seen from the previous process, both policy and the testing of that and any controls are an essential component of developing a secure environment. The most effective way to achieve this is through the SMART process.

Specific

When creating policy, many organizations have the idea that everything should be in the one document. This method results in huge policy documents that can exceed 100 pages. Worse, it cannot be expected that an employee will actually ever read this document. On top of this, large integrated policy documents are extremely difficult (if not impossible to maintain). Having to go to the board with a 100+ page document for every minor change will soon lead to a hostile attitude towards information security.

Detail each component of the security infrastructure separately.

Specific applies to having a collection of separate system and issue specific policies. Each policy should fully cover one, and only one, discrete issue and use links to refer to related policies! An excellent test to determine if the policy satisfies the requirements of specificity is to determine if procedures can be directly developed using it as guidance.

The question should be asked when developing or auditing policy; "*Is the policy specific enough to give appropriate guidance*?" The check for appraising the level of specificity used in a policy is to ensure that the policy is suitably detailed to permit procedures and checklists to be appraised against any procedure that is designed to enforce the policy.

In auditing policy or procedures, SMART also applies. For a policy or procedure to be specific, it needs to be able to provide an answer to the following questions:

- Who performs the procedure?
- What is the procedure?
- When is the procedure done?
- Where is the procedure done?
- How do we know the procedure is done?

Measurable

It is essential that any controls (including policy and procedures) are auditable and that they may be tested and accredited. When designing policy, consideration needs to be made to address how the policy will be tested. This allows you to ensure it is effective.

When implementing procedures to effect policy, give consideration to record sizes, times and logging. How are these controls to be tested and measured?

To be measurable, a policy needs to be specific so that a user can tell if they are following its guidance and remaining compliant.

Achievable

The best policy and security architecture in the world means nothing if it cannot be both implemented and maintained. Ensure that you have the resources to achieve your objectives.

Achievable relates to whether the objectives can be completed in a reasonable time, cost and effort. Policies that state you needed to do something, or needed to not do something when it just was not going to happen are common. If you cannot enforce a policy, it is worthless. For instance, take "No personal Internet Use Allowed" policies. If the organization also has a policy of not monitoring employee Internet usage, then the first policy can never be effective.

Realistic

Evidence matters. Collect facts and make pragmatic judgments based on what is achievable with the time, budgetary and staff/knowledge constraints that face the organization.

Realistic has a number of meanings when considered against policy development. For instance:

- **Organizational security posture**. Is the policy realistic for the organization’s culture?
- "**Policy tax**". If policy and procedures are considered to be too burdensome, users will find ways to not do them. Users are great at discovering control flaws when they want to do something that is forbidden.
- **Cost**. Setting a policy that states the organization will base a DR site on the moon and setting a budget of $100k is unrealistic to say the least.
- **Staff**. Setting a policy that states that the organization will monitor 250 systems with one full time employee with no budget for tools is doomed to failure.

Time-based

Developing policy is a strategic task, implementing them is tactical. This means that policy need to meet the challenges that inevitably will arise using a project based mindset. Work to time constraints and deadlines and ensure that any events are recorded as they have occurred. Also consider the following questions when assessing policy:

- When is the policy to be updated and how long is it effective?
- When was the policy last updated?
- How often should a control apply and for how long?

Time is a common consideration that is missed. It is one of the main areas that are in need of improvement when developing policy. It is common for organizations to develop policy that ignores the time component all together.

It is common to find a policy that states:

“**All user accounts associated with an employee must be disabled following the termination of that employee in a manner that ensures they are made inactive**”.

Other than being written in a formal language that makes the policy less than clear, there is nothing to determine when the change needs to occur. Should this be implemented:

- Within 15 minutes
- Within 2 weeks?
- In the same financial reporting year?

It is easy to see that the policy example is difficult to enforce. Any system administrator that is pulled up by management for not complying with the policy could simply state “I planned to do it tomorrow”. Who knows, maybe they did plan to do it tomorrow.

Time statements improve the effectiveness of policy and make it possible to test and also provide guidance as to when they need to be updated.

The Policy Lifecycle Process

Figure 6.1 illustrates a policy lifecycle process developed by SANS (A link to the SANS Policy primer is provided later in the chapter). This process starts at the left top corner with a policy review and request process. This either triggers an update to an existing policy, or the need to develop a new policy.

If the intent of an existing policy is changed by an update, it should be routed through the standard SME[1] and department review just as new policies are reviewed. The policy review process often involves several different parts of the organization such as HR and legal, in addition to the corporate security team. Once a policy has been reviewed and approved by the different departments, it should be approved by a steering committee or policy lead. After the policy is approved, there is a need to publish on an internal website and communicate out to the user community. In some cases, policies may need to be translated into different languages for global corporations or passed along to vendors and partners.

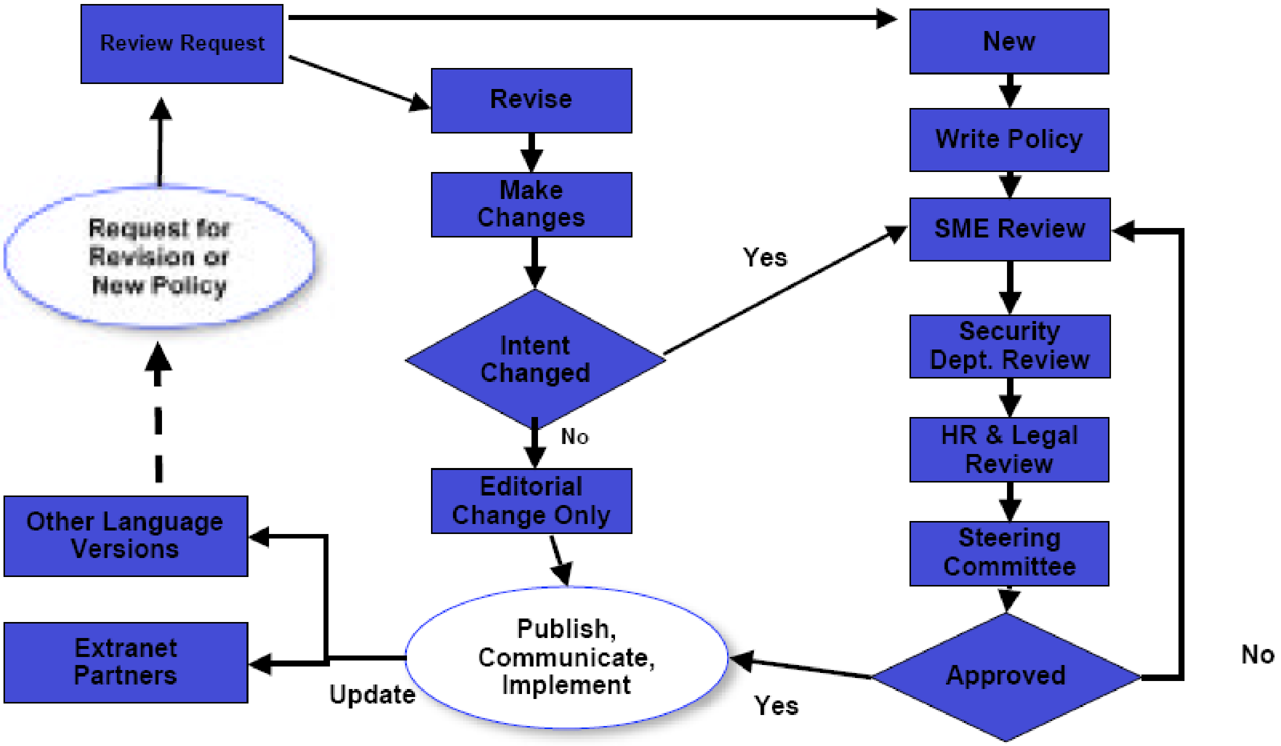


Figure 6.1 The Policy lifecycle process

A revision to a policy changes the policy intent if the original scope is affected or if a specific activity is changed.

What's what

[1] Subject Matter Expert (SME)

So what is the difference between all these documents? Policy, procedures, standards and frameworks all seem to have the same goals, but they are different none the less. The policy infrastructure comprises of policy, standard, and guideline documents. Policy is characteristically where the rules are laid down. It is a document that specifies the conventions that are to be enforced within the organization.

When applied to information security, policies cover a framework from the high level policy that forms the vision for security within the organization through to issue-specific policies that are focused on a single outcome. An Acceptable Use Policy (AUP) for instance is designed to set the conventions that are deemed appropriate to allow the safe use of the computing facilities within an organization.

Standards are characteristically a set of system-specific or procedure-specific requirements that need to be complied with universally throughout the organization.

For example, the organization may decide to implement the Windows level 1 benchmark from the Center for Internet Security (www.CISecurity.org) for XP as a standard that describes how to harden Windows XP workstations that are to be issued to users on the internal network. All users and external consultants would be required to adhere to this standard if they want to use Windows XP on the internal network segment.

A guideline is characteristically a set of system-specific or procedure-specific suggestions designed to direct staff to following best practice. Guidelines are not requirements and are not enforced even if they are stalwartly recommended. To be effective, security policies need to make frequent references to the standards and guidelines that exist and are accepted within the organization.

NOTE

Security policy should change very infrequently.

Procedures are used to incorporate the technical aspects of an organization’s infrastructure that change too regularly to be contained within policy.

Mission, Vision and Values Statements

Just as the organization should have a Mission or Vision statement aligned to what its business goals are, it should also have them for IT and information security. Having a mission to comply with the laws, regulations, and organizational policy makes it more likely that this will occur and is essential if a culture of security is to be introduced.

Vision and mission statements are very different documents. A vision statement sets the goals of the organization at a high level. The vision needs to state what the organization envisions, in terms of growth, attitude to risk, cost, values, employees, etc. A component of the vision statement includes the development of a mission.

The Mission Statement

The mission statement is (or at least should be) a concise statement of the organization’s strategy. It is developed from the perspective of a desired outcome and it needs to be aligned to the vision statement.

The mission should answer three questions:

1. What do we do and why?
2. How do we do it?
3. For whom do we do it?

In assessing high level policy it is essential to test whether the policy is aligned to the mission of the organization. For instance, Google used to have a mission statement that said "*Do no evil*". A policy that states "*We will track down and destroy any attacker who even pings our network*". It is simple to see that the goal and the policy are not linked.

The information technology and security teams or departments should have there own mission statement. This should be a simple statement of purpose known by every member of the division. This:

- Provides a "reason for being".
- Provides clarity and focus and makes choices.
- Is clear and concise.
- Should be accepted by the wider organization.

The Vision Statements

The vision statement outlines what the organization wants. This is what it wants to be and how it wants to be perceived by others. A vision statement is:

- A plan for the future;
- A source of inspiration.
- The place to go when in need of clear decision-making criteria.
- The source to ensure that policy aligns with the destination set by the organization.

Vision Statement expresses the destination of the organization in a manner that builds commitment:

1. It creates a sense of desire and builds commitment.
2. Paints the ideal future.
3. Is an expression made in terms of hope.
4. Is united with the values of the organization.

A Statement of Values

Many organizations also develop a set of ethical principles that are designed to guide the organization. These principles are the statement of values. This document should be used as guidance when developing policy.

This can also be called an organizational code of ethics.

Framework

To either assess or develop policy, they need to be set in a framework that allows for a structured approach to understanding and implementing issues individually. Start by developing a root policy (or top of the policy chain).This can be the mission statement, or can be based directly from a regulatory requirement or from legislation that the organization is required to adhere to. The framework can be different for different policies.

The framework derives from asking the question, "*Is there higher level guidance outside of this organization that this organization should follow?*" Next reflect on the overall security posture within the organization, the various levels of policies that already exist (if any), and the critical policies and procedures that both need to be in place and that have already been implemented.

Policy

A policy is typically a document that outlines specific requirements or rules that must be met. A policy is a intentional plan of action to guide decisions in order to achieve a desired rational outcome.

Policy is a formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. Policy attributes include the following:

- *Require compliance (they are mandatory)*
- *Failure to comply results in disciplinary action*
- *Focus on desired results, not on means of implementation*
- *Further defined by standards and guidelines*

Policy Levels

Policy should be a part of a framework. This starts with a high level policy that sets the overall requirements and should go into specific policy for individual issues that are faced by the organization.

High Level Policy

This is the document that guides the development of the policy framework. It should be authorized at board level (or as high as possible).

A critically task is the establishment of a security documentation baseline. The baseline is the foundation for evaluating the security policy for effectiveness and accuracy. Security documentation can be expected to vary across every organization(although several components will be similar).

High level documents such as a mission statement define what customers, suppliers, and employees should be able to anticipate from the organization

Issue specific and System Specific Policy

At the other end of the policy framework are those policies that are specific to a single system or issue.

Standard

A standard is a procedure or a set of specific requirements that must be met by everyone.

Information is one of if not the most valuable resource held by an organization. It needs to be protected. Standards need to be applied to all characteristics that are commonly associated with the handling of information and information systems. This needs to be done in a manner that is aligned to the Information Security Policy. A collection of minimum standards that must be applied when handing organization's information assets should be developed in a manner that complements the security policy.

Standards can be depicted as a workable and generally specific statement of the expectations or controls that the organization has mandated. The objectives of an organization's standards should be to define a set of requirements that are designed to end in the implementation of a minimum level of security for each information classification category. Standard should provide developers of systems with a minimum standard required to secure new and current applications.

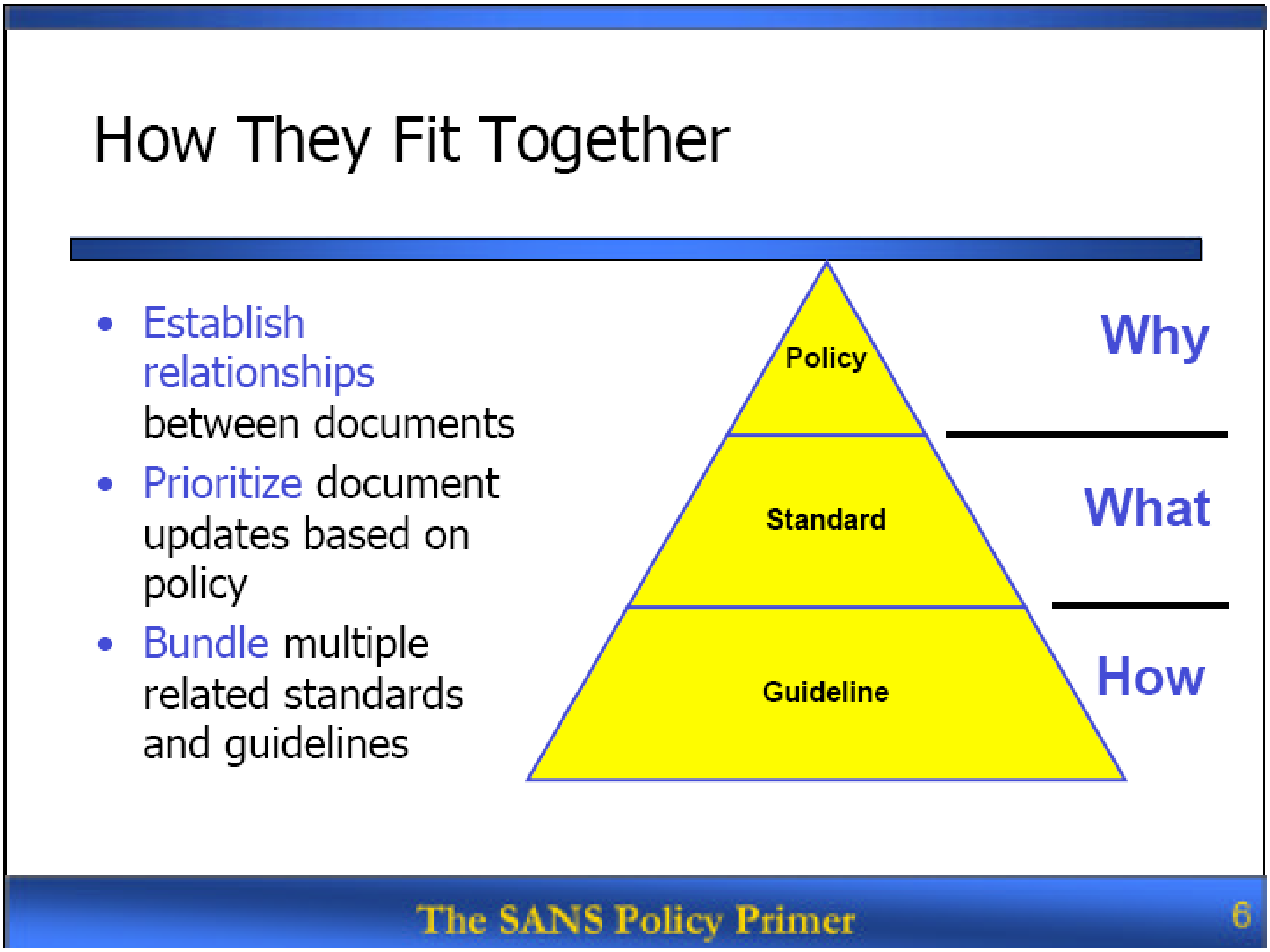
The standards should be divided into the following areas of information systems:

- General
- Information Classification Categories

Guideline

A guideline is a collection of system-specific or procedural-specific recommendations for best practice, e.g., Microsoft Security Templates

A guideline is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization.



How They Fit Together

- Establish relationships between documents
- Prioritize document updates based on policy
- Bundle multiple related standards and guidelines

Policy

Standard

Guideline

Why

What

How

The SANS Policy Primer

6

Figure 7.1 Taken from "A Short Primer for Developing Security Policies" (SANS Policy Project)

Process or Procedure

Procedures are a control that is designed to ensure that the policy is effected. For instance, a procedure could set the controls in place that are designed to ensure that only those authorized to access a systems can do so. Procedures are a means of supporting the objectives of the security policy and a method of implementing it within the organization. Some procedures commonly defined within an organization include:

- Procedures for obtaining access to a system and being issued a USERID and password;
- Logon Procedures;
- Procedures for password controls;
- Procedures to handle incidents such as a security breach; and
- Procedures to deal with malware (such as a computer virus or worm);

Interpreting Policy as an Auditor

Assessing policy is analogous to assessing a site. Use the same methodology to assess a system or a policy:

- Establish a baseline framework
- Assess and repair critical policies
- Assess and repair one at a time after you assess critical policies

Look for prior work as well. It is never advisable to rebuild the wheel from scratch. The following documents can help in distinguishing reality from perception. The mission statement is an organization wants to look like. The security posture is what things are really like. The following documents aid in determining this difference:

- Assessment documents (prior audits, risk reports, vulnerability scans and penetration tests),
- System, network and security device configuration and operational documents,
- Operational security, network and system administrator task procedures, and
- Any other policies and procedures.

The security posture or the aspects of corporate culture that cover security are for the most part significant when attempting to develop, implement, or enforce security policy. Corporate culture always exists, whether it is intentionally cultivated or it develops organically. Senior management can attempt to shape corporate culture by imposing corporate values and standards of behavior that specifically reflect the objectives of the organization, however, the extant internal culture within the workforce can subvert this process.

A conscious effort to establish a culture that embraces security should be based on a process of communicating the message through:

- Vision statements
- Mission statements
- Doctrine or Core values
- Frequent internal writings on related topics
- Awareness sessions

The key to establishing values is frequent, consistent and repeated communications.

No organization is homogeneous. Within an organization, divisions will also have their own cultures and hence different security postures. To be successful developing, implementing and enforcing security policy, a leader needs to be sensitive to the character of the departments as well as the overall organization.

Assessing the security posture and implementation of a culture of security requires looking for evidence of senior management’s involvement in the cultural engineering exercise. Does the organization even have a security mission statement?

Simple steps to assess the security posture

To ensure compliance of systems with organizational security policies and standards, the security of IT systems should regularly reviewed and checked.

System Audit Considerations

To minimize interference either to or from the system audit process controls should be implemented to safeguard the operational systems and audit tools for the duration of any system audit. Some of the policy questions to ask in an audit (from SANS) that may be used when determining the effects of policy are included below:

- *Do the managers know the mission statement*
- *Wandering around the organization without a badge to see if anyone challenges you.*
- *Calling someone to see if they are willing to send you documents that have not been approved for public release.*
- *Run a password assessment tool, and if half the passwords are named after their favorite sports teams, that's a bad sign.*
- *A few simple questions can help determine the level of security controls at a site. Some to ask follow:*
- *Evaluate the commitment of senior management to physical, information, and intellectual property security. At the same time, evaluate the level of risk senior management is willing to accept. If there is no commitment from senior management, there cannot be a culture of security.*
- *Evaluate the presumption of privacy, including phone and network monitoring.*
- *Do employees have a reasonable expectation that the files on their computers and their phone and Internet communications are protected?*
- *Does company policy allow random physical searches, and is there an active search program?*
- *Is the perimeter configured to allow all connections initiated inside the organization?*
- *What is the level of employee awareness of security practice?*
- *Do employees know procedures for developing and protecting information systems?*
- *Is the employee able to add software or modify settings on the desktop system?*

- *Are administrators able to make changes without going through a formal configuration-management approval program?*

- *Can the internal auditors name a dozen technical security protective or detective controls without looking for them?*

Understand where the organization is on the path towards developing a culture of security, and this will better help in differentiating the difference from perception and reality. This is necessary if a baseline that may be used to evaluate policy is to be established. This process most commonly starts with a mission, vision statement or high level policy that communicates the core vision. Communication and the dissemination of the vision is a slow process that never ends if it is to remain effective.

Security documentation evaluation

There are two main approaches to evaluating policy:

- Start by looking over all of the operational documentation that is available and then examine these documents to see if they are covered by policy.

- Look at the existing policy set to see if it is complete and if there is sufficient documentation to support the policy.

Using either approach will help in identifying missing documentation that needs to be developed.

Various levels of policy and their functions

Enterprise-wide or corporate policy is the highest level of policy and consists of a high-level document that provides a direction or thrust to be implemented at lower levels in the enterprise. The ISO 17799 (ISO 27002) approach to this, for information security, is a letter of endorsement from senior management. This policy must exist to properly assess lower level policy. If this policy does not exist, begin work to create this policy document and get it approved before attempting to assess lower level policy. This enterprise or corporate level security policy is the demonstration of management's intent and commitment for the information security in the organization. This should be based on facts about the criticality of information for business, as identified during our assessment and evaluation of security posture (SANS).

The security policy statement should strongly reflect the management's belief that if information is not secure, the business will suffer. The policy should clearly address issues like:

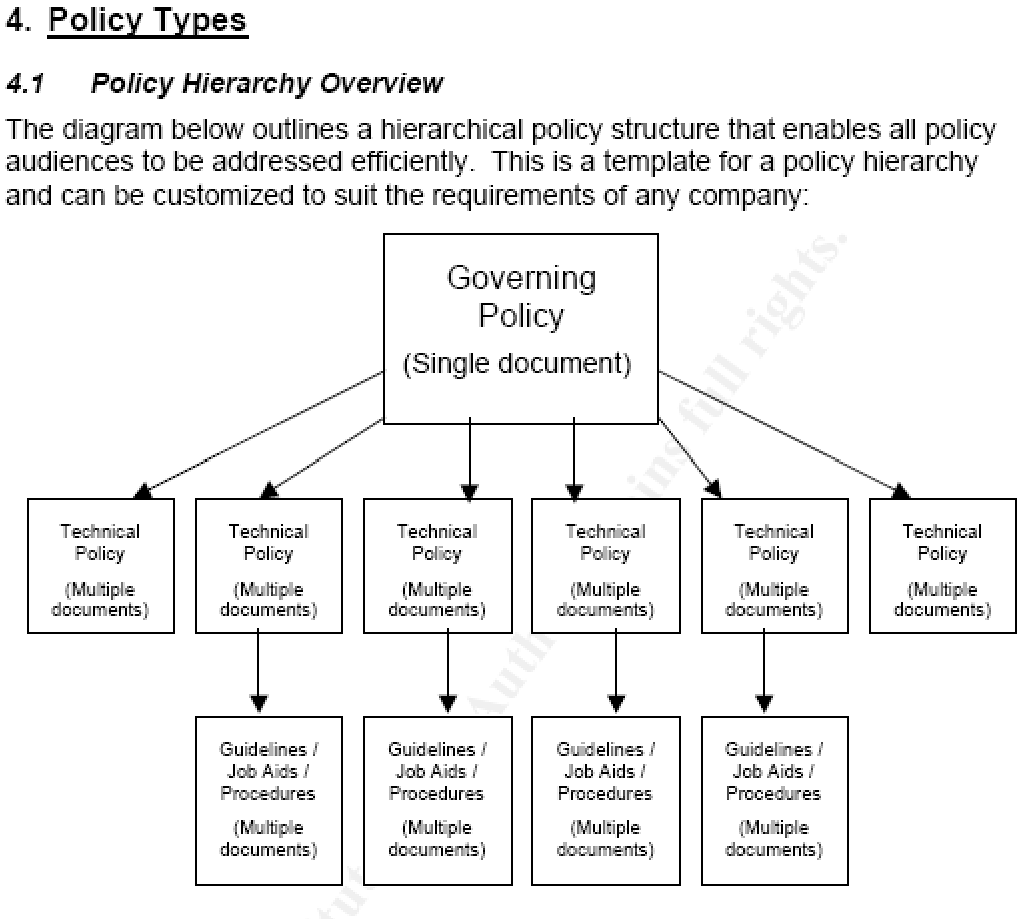
- *Why information is strategically important for the organization?*

- *What are business and legal requirements for information security for the organization?*

- *What are the organizations' contractual obligations towards security of the information pertaining to business processes, information collected from clients, employees, etc.?*

- *What steps the organization will take to ensure information security?*

A clear and concise security policy provides the bearings that the information security efforts of the organization will follow. It also helps to instill confidence in the various stakeholders within the organization.



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:

Figure 7.2 Taken from “Information Security Policy - A Development Guide for Large and Small Companies” (SANS Policy Project)

The Managing Director or Chief Executive Officer of the organization should issue or act as the approving authority of the security policy statement, to build the momentum toward information security and set clear security goals and objectives.

A framework should be based on the concept of policy hierarchy. Start with the organization’s mission statement and corporate policy in hand, and then proceed (prepared) to assess the lower level policies. The following are categories of policies that should be considered:

- **Division-wide policy.** Typically, this consists of an amplification of enterprise-wide policy as well as implementation guidance. This level might apply to a particular region of a national corporation.

- **Local policy.** This policy contains information specific to the local organization or corporate element.

- **Issue-specific policy.** Policy related to specific issues, can include firewall or antivirus policy.

- **Security procedures and checklists**. Local standard operating procedures (SOPs) are derived from security policy.

Security policy may exist on some levels and not on others. You might not need a division-wide policy for every division. Documents interact and support one another and generally contain many of the same elements. This is almost always true in a multi-national organization. For example, the legal framework is radically different in France, Australia, and the United States. This could have a profound impact on the specifics of policy. However, the policy attempts to achieve the same effect in all three countries, so the similarities probably exceed the differences. In a typical organization, policy written to implement higher-level directives may not relieve (waive) any of the requirements or conditions stipulated at a higher level. After all, we really can't have the data center manager overturning policy signed by the Chief Executive Officer of the company. In addition, security policy must always be in accordance with local, state, and federal computer-crime laws and regulations. As an example, the security policy for a hospital in the United States would fall within the regulatory guidance of HIPAA.

The framework for issue and system specific policy

If the framework for issue and system specific policy are the issues themselves (acceptable use, password etc), then the structure is the template that contains the sections of the policy. By choosing a template, an organization achieves consistency in their policy which is a step towards higher quality. Typical sections of issue-specific policy can include the following:

Purpose

The purpose is the reason that the policy exists. Once an organization has the majority of their policies developed, the reason for most new policy is a technology change or an unexpected event. If it is an unexpected event it is usually because an individual did something or asked something no one had thought about. In those cases, sensitivity and care should be used in writing the purpose statement as not to draw attention to the individual.

Background

If you have a purpose statement, do you always need a background? No! This would be a secondary or optional policy section. However, if the policy is going to impact people who fall under its scope, this can be an opportunity to expand on the "why". People are more likely to follow policy when you give them the background, the reasons the policy has been put into place.

Overview or executive summary

This is also a secondary or optional policy section, since this section is often used to summarize the policy body, great care must be taken to make sure the words in this section do not contradict or modify the body of the policy. If you are writing short issue or system specific policies you probably do not need this section.

Related documents

Any documents (or other policies) that affect the contents of this policy. This is one of the strongest reasons to consider posting policies as html documents.

Cancellation

Any existing policy that is cancelled when this policy becomes effective. This can be incredibly important. If you type "policy cancellation" into Google you will see insurance policy cancellation for the entire first page. But cancellation (especially by superseding) is an important concept in policy management.

Scope

The range of coverage for the policy. (To whom or what does the policy apply?) The knee jerk response we often see is everybody, but is that really correct? Most organizations have a large number of contractors providing services and the primary document that controls what does and does not apply to those contractors is the contract and service level agreement.

Policy statement

The actual guiding principles or what is to be done. The statements are designed to influence and determine decisions and actions within the scope of coverage. The statements should be prudent, expedient, and advantageous to the organization.

The policy statement, or body of the policy, identifies the actual guiding principles or what is to be done. The statements are designed to influence and determine decisions and actions within the scope of coverage. The statements should define actions that are prudent, expedient, or advantageous to the organization. There is a lot of bad policy out there, so let's consider what the security manager can do to guide the creation of good policy that people will actually read and follow.

Action

States the actions that are necessary and when they are to be accomplished. While this is not needed on all policy, this should be in your checklist. Many policies function better if someone is assigned to do something; and, this is particularly true with system specific policy.

Responsibility

Who is responsible for what? Subsections might identify who will develop additional detailed guidance and when the policy will be reviewed and updated. This is clearly related to the action section.

Compliance or enforcement

This is where the boiler plate "Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment" is often inserted. However, one thing to think about for policies that apply to important, but fairly minor, issues in the overall scope of things, is a specified disciplinary action.

Information Security leaders can improve the quality of their issue and system specific policies by establishing a template to ensure policy has all the sections that it should. In addition, don't assume that policy authors understand all the implications or uses of the sections of policy simply by their name.

Identifying Preventive, Detective and Corrective Controls

The purpose of a security policy is to provide management direction and support for Information Security within an organization.

An organization's management should set a clear direction and demonstrate their support for information security through the issue of an Information Security Policy. The establishment of an Information Security Policy should be the first objective in the development of your organizations Security Infrastructure as it provides the foundation on which it will be built.

Preventive Controls

These are controls that are designed to stop an incident from occurring in the first place. Some examples are:

- Anti-virus,
- Firewalls,
- Authentication

Detective Controls

These are controls that are designed to discover when something has gone wrong. Detective controls include:

- IDS
- Logging and monitoring
- Audit

Corrective Controls

These are controls that are designed to fix a problem that has been detected. Some examples include:

- Incident handling procedures
- BCP and recovery procedures

Developing a Security Policy

The aim of this process is to develop policies and procedures that are designed to meet the business needs of the organization. This process should provide a framework under which all security architecture design, implementation and management can be accomplished.

Security policy and procedures should be created from information collected from the organization's and its staff. To determine what your security requirements are, is best achieved by a combination of:

- The results of an Information Asset Inventory,
- Interviews with Information Asset Owners,

- Interviews with IT Security Staff, and
- Interviews with organization Managers.

The next stage is to develop a corporate security policy that will contain, at a minimum:

- A definition of information security with a clear statement of management's intentions,
- An explanation of specific security requirements including:
    - Compliance with legislative and contractual requirements
    - Security education, virus prevention and detection, and business continuity planning
- A definition of general and specific roles and responsibilities for the various aspects of your information security program
- An explanation of the requirement and process for reporting suspected security incidents, and
- The process, including roles and responsibilities, for maintaining the policy document.

Begin by talking about the issue

Before even starting to write policy, find some people and discuss what you want to achieve. Talk about the tradeoffs:

- Could the policy be more liberal or stricter,
- Could it be more specific or more liberal?

There are two principal reasons to do this:

- The aim is to get buy in from the stakeholders. Asking people's opinion before sending them a draft allows you to determine the views of others and also to demonstrate that you care about their opinion and want their feedback. This gets people involved.
- By discussing the policy out loud you begin to collate the concepts into a logical readable issue.

The use of the English language in Policy should be SIMPLE

Policy should be simple. For most organizations it should be targeted somewhere between 6th and 9th grade mastery of the English language.

Overly wordy policies with impressive sounding words are commonly misunderstood.

Keep the language used in writing policy Simple!

Policy should be evaluated on clarity and conciseness

When evaluating policy, assess it from the perspective of the consumer. In this case this is the individual who needs to read, understand, and follow the policy.

The policy simply has to be clear and concise.

If a user starts to read something they do not understand, they tend to go on to something else.

Policy Areas to be considered

A good security policy should contain several sections such that it is easier to update. Some examples of the sections that could be contained within a security policy are displayed in the following sections.

Identification and Authentication

Identification for the purposes of these standards relates to the way an individual is identified to the system. Logon security is the method commonly used to identify the user accessing the system.

The purpose of authentication is to verify that the person trying to access a system are who they say they are. Authentication is typically verified by the user supplying a password. Other methods of Authentication may be defined as well.

Access Control

Access controls are provided by software protection measures or procedures to control access to system applications and information according to an organization’s specified rules.

Access controls are prevention measures designed to:

- prevent and minimize threats;
- ensure only authorized users have access to systems and information; and
- ensure information is protected according to the classification levels.

Software Security

Software security concerns the methods used in controlling software that is used to run the operating system or utility software that supports the running of the operating systems and applications.

Software security refers to the protection of the programs that are either bought from an outside vendor or are created in-house by the user.

In order to ensure integrity of information, transaction processing should conform to the ACID properties as defined below:

- **Atomicity** A transaction involves two or more discrete pieces of information. Ensures that either all pieces of the transaction are committed or none are.

- **Consistency** Requires that a transaction either create a new and valid state of data or, upon failure; return all data to its previous state.

- **Isolation** While a transaction is in process, and is not yet committed, it must remain isolated from any other transaction.

- **Durability** That committed data is saved by the system even in the event of failure. When the system comes back up, the data is available in its correct state.

Physical Access Control

Physical security measures are intended to protect an organization's computer related physical environment from potential hazards, whether people created or natural, that may impact an organization's ability to deliver services to customers or personnel

Monitoring and Review

The security environment must be auditable and regular audits must be conducted by the Internal Audit group and management to ascertain the level of compliance with the security policy, standards and procedures. It is essential that processes are in place to provide audit trails of authorized and unauthorized access to systems.

Incident Management

Security breaches can be defined as a deliberate action to circumvent or defeat security controls.

The security environment must be auditable and regular audits must be conducted by an external third party or the Internal Audit group and management to ascertain the level of compliance with the security policy, standards and procedures.

Policy Frameworks

ISO 17799:2005 (ISO 27002) is a good starting point in the process of developing a security policy document, as it provides a guideline to best practices for security processes and mechanisms. There are 12 areas in the standard containing many more groups and over 100 security control areas. One method to create a policy involves tailoring these controls to develop a set of policies and standards that will be appropriate for the level of risk the organization is willing to assume based on its business requirements.

An ISO 17799 Summary

The following is a brief introduction to the various headings in the ISO17799:2005 (ISO 27001) control framework for security. ISO 17799 starts with the definition of the **Scope** and also the **Terms and definitions** that are used throughout the document.

Each of the other sections are mentioned below.

3. Information security policy

To provide management direction and support for information security, top management should set a clear direction and demonstrate their support and commitment to information security through the issue of a documented information security policy available to the entire organization.

4. Security organization

This section covers the following controls:

4.1 Information Security Infrastructure

4.2 Security and Third Party Access

4.3 Outsourcing

Information security infrastructure

To manage information security within the entire organization, a management framework should be established to initiate and control the implementation of information security.

Security of third party access

To maintain security of organizational IT facilities and information assets, accesses by third parties should be controlled.

5. Assets classification and control

This section incorporates the controls that cover how an organizations assets should be classified.

Accountability for assets

To maintain appropriate protection of organizational assets, all major information assets should be accounted for and have a nominated owner.

Information classification

To ensure the information assets receive an appropriate level of protection, security classifications (CIA) should be used to indicate the need and priorities for security protection.

6. Personnel security

Staff are one of the most difficult and also most frequently overlooked aspects of organizational security.

Security in Job Definition and Resourcing

To reduce the risks of human error, theft, fraud or misuse of facilities, security should be addressed at the recruitment stage, included in job descriptions and contracts, and monitored during an individual's employment.

User Training

To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work, they should be trained in security procedures and the correct use of IT facilities.

Responding to Incidents

To minimize the damage from security incidents and malfunctions, and to monitor and learn from them, incidents affecting security should be reported through management channels as quickly as possible.

7. Physical and Environmental Security

If the physical security is not maintained, logical security is doomed to fail.

Secure Areas

To prevent unauthorized access, damage and interference to the business normal course, all facilities supporting critical or sensitive business activities should be housed in secure areas.

Equipment Security

To prevent loss, damage or compromise of assets and interruption of business activities, equipment should be physically protected from security threats and environmental hazards.

8. Communications and Operations Management

This section covers the daily operations and general running of systems.

8.1 Operational Procedures and Responsibility

8.2 System Planning and Acceptance

8.3 Protection against Malicious Software

8.4 Housekeeping

8.5 Network Management

8.6 Media Handling and Security

8.7 Exchanges of Information and Software

Operational Procedures and Responsibilities

To ensure the correct and secure operation of computer and network facilities, responsibilities and procedures for the management and operation of all computers and networks should be established.

System Planning and Acceptance

To minimize the risk of systems failures, advance planning and preparation are required to ensure availability of adequate capacity and resources.

Protection from Malicious Software

To safeguard the integrity of software and data, precautions are required to prevent and detect the introduction of malicious software.

Housekeeping

To maintain the integrity and availability of IT services, housekeeping measures (back-up of data, log of events, environment monitoring) are required.

Network Management

To ensure the safeguarding of information in networks and the protection of the supporting infrastructure, the security of computer networks which may span organizational boundaries and may include public networks, require special attention.

Media Handling and Security

To prevent damage to assets and interruptions to business activities, computer media should be controlled and physically protected.

Data and Software Exchange

To prevent loss, modification or misuse of data, exchanges of data and software between organizations should be controlled.

9. System Access Control

This section covers the controls on how the system is accessed and the authorization controls over objects.

Business Requirement for System Access

To control access to business information, access to computer services and data should be controlled on the basis of business requirements.

User Access Management

To prevent unauthorized computer access, there should be formal procedures to control allocation of access rights to IT services.

User Responsibilities

To prevent unauthorized user access, the cooperation of authorized users is essential for effective security.

Network Access Control

To ensure that connected users or computer services do not compromise the security of any other networked services, connections to networked services should be controlled.

Computer Access Control

To prevent unauthorized computer access, access to computer facilities should be controlled and restricted to authorized users.

Application Access Control

To prevent unauthorized access to information held in computer systems, logical access control should be used to control access to applications and data.

Monitoring System Access and Use

To detect unauthorized activities, systems should be monitored to ensure conformity to access policy and standards.

10. Systems Development and Maintenance

This section is designed to development of new systems and the update of existing ones. It includes a number of considerations:

10.1 Security Requirements of Systems

10.2 Security in Application Systems

10.3 Cryptographic Controls

10.4 Security of System Files

10.5 Security in Development and Support Processes

Security Requirements

To ensure that security is built into IT systems and applications, security requirements should be identified and agreed prior to development.

Security in Applications

To prevent loss, modification or misuse of user data in applications, appropriate security controls, including audit trails, should be designed and implemented.

Security of Operational Files

To ensure that IT projects and support activities are conducted in a secure manner, access to operational system files should be controlled.

Security in Development and Support Environments

To maintain the security of application system software and data, project and support environments should be strictly controlled.

11. Business Continuity Planning

ISO 17799 (27002) addresses the need to ensure that systems are maintained with an eye to continuity.

Aspects of Business Continuity Planning

To counteract interruptions of business activities, business continuity plans should be available, tested and maintained to protect critical business processes from the effects of major failures or disasters.

12. Compliance

This section covers:

12.1 Compliance with Legal Requirements

12.2 Reviews of Security Policy and Technical Compliance

12.3 System Audit Considerations

Compliance with Legal Requirements

To avoid breaches of any statutory, criminal or civil obligations and of any security requirements, the design, operation and use of IT systems may be subject to statutory and contractual security requirements.

The SANS Security Policy Project

This project is the first place to go if you need to find a template to implement a new policy.

There is no cost for using these resources. On their website, SANS have provided numerous consensus policies and policy templates. These can be used to get an organization's security programs updated to reflect 21st century security requirements. It also offers a primer for those new to policy development and specific guidance on policies related to legal requirements such as the HIPAA guidelines.

This page is a work in-progress and the policy templates are "living" documents. The policies on the site are brief, easy to read, feasible to implement, and effective. See the site (http://www.sans.org/resources/policies/) for more details.

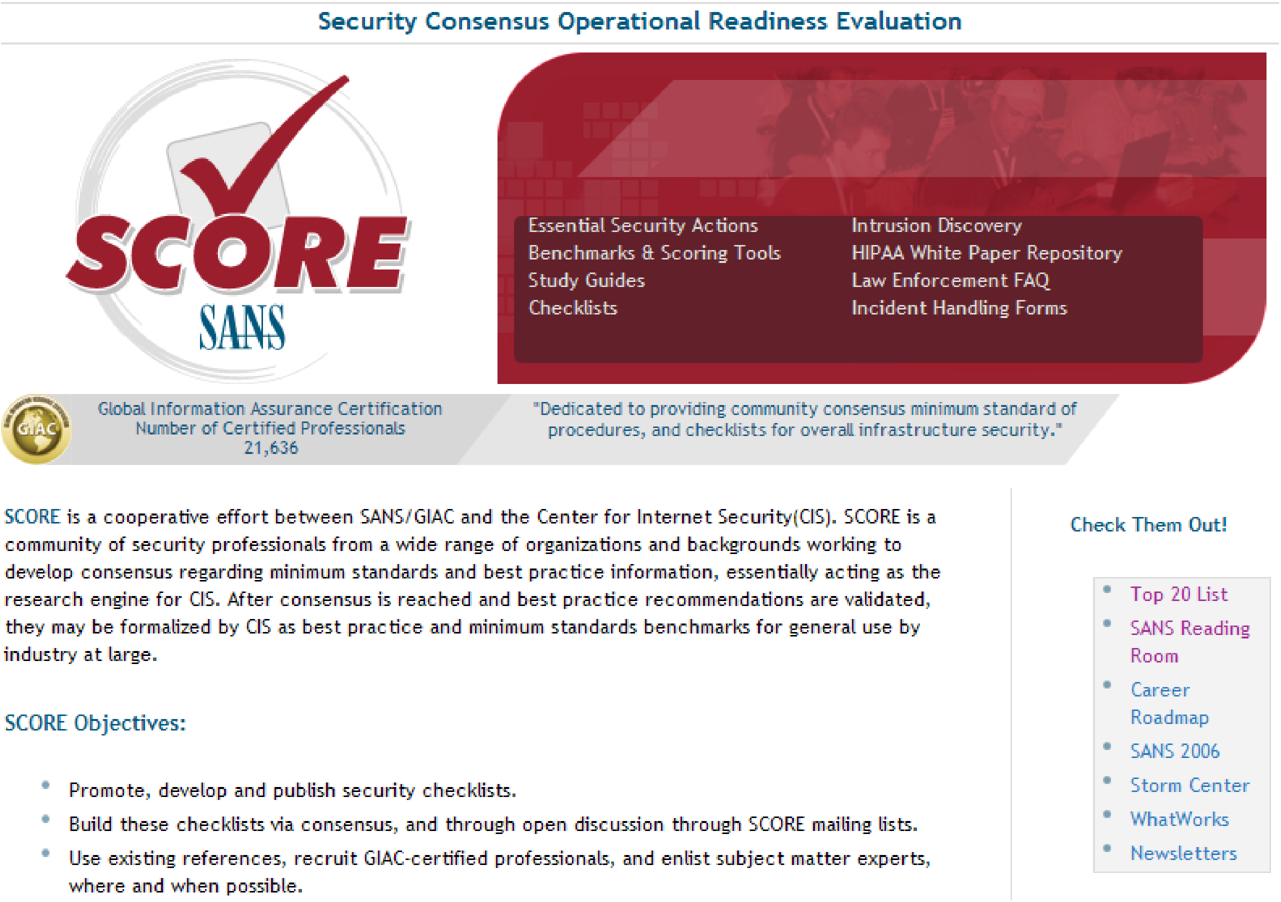
Need an Example Policy or Template?

SANS provides a number of security policies and templates that can be an effective method of starting a policy project within an organization. These policies were developed by a group of experienced security professionals in government and commercial organizations. Each policy has been subjected to a vigorous approval process.

Some tips about these policies. Anything that is in <angle brackets> should be replaced with the appropriate name from your organization. The term "InfoSec" is used throughout these documents to refer the team of people responsible for network and information security. Replace "InfoSec" with the appropriate group name from your organization. Any policy name that is in italics is a reference to a policy that is also available on this site.

SANS SCORE

SANS SCORE (Security Consensus Operational Readiness Evaluation) should be the first stop when learning about security policy.



Security Consensus Operational Readiness Evaluation

Global Information Assurance Certification
Number of Certified Professionals
21,636

"Dedicated to providing community consensus minimum standard of procedures, and checklists for overall infrastructure security."

SCORE is a cooperative effort between SANS/GIAC and the Center for Internet Security(CIS). SCORE is a community of security professionals from a wide range of organizations and backgrounds working to develop consensus regarding minimum standards and best practice information, essentially acting as the research engine for CIS. After consensus is reached and best practice recommendations are validated, they may be formalized by CIS as best practice and minimum standards benchmarks for general use by industry at large.

SCORE Objectives:

- Promote, develop and publish security checklists.
- Build these checklists via consensus, and through open discussion through SCORE mailing lists.
- Use existing references, recruit GIAC-certified professionals, and enlist subject matter experts, where and when possible.

Figure 7.3 SANS Score. The consensus standard

Example Policy - SANS InfoSec Acceptable Use Policy

The following policy is an example of the many freely available templates that have been developed as a part of the SANS Security Policy project. This document is included with permission from SANS.

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Overview

InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <Company Name>'s established culture of openness, trust and integrity. InfoSec is committed to protecting <Company Name>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of <Company Name>. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every <Company Name> employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at <Company Name>, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by <Company Name>.

4.0 Policy

4.1 General Use and Ownership

While <Company Name>'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of <Company Name>. Because of the need to protect <Company Name>'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to <Company Name>.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.

For security and network maintenance purposes, authorized individuals within <Company Name> may monitor equipment, systems and network traffic at any time, per InfoSec's Audit Policy.

<Company Name> reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.

All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.

Use encryption of information in compliance with InfoSec's Acceptable Encryption Use policy.

Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.

Postings by employees from a <Company Name> email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name>, unless posting is in the course of business duties.

All hosts used by the employee that are connected to the <Company Name> Internet/Intranet/Extranet, whether owned by the employee or <Company Name>, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by <Company Name>.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <Company Name> or the end user does not have an active license is strictly prohibited.

Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Using a <Company Name> computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

Making fraudulent offers of products, items, or services originating from any <Company Name> account.

Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.

Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

Circumventing user authentication or security of any host, network or account.

Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Providing information about, or lists of, <Company Name> employees to parties outside <Company Name>.

Email and Communications Activities

Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

Unauthorized use, or forging, of email header information.

Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Use of unsolicited email originating from within <Company Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>'s network.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.4. Blogging

Blogging by employees, whether using <Company Name>’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of <Company Name>’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>’s policy, is not detrimental to <Company Name>’s best interests, and does not interfere with an employee's regular work duties. Blogging from <Company Name>’s systems is also subject to monitoring.

<Company Name>’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>’s Confidential Information policy when engaged in blogging.

Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of <Company Name> and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by <Company Name>’s Non-Discrimination and Anti-Harassment policy.

Employees may also not attribute personal statements, opinions or beliefs to <Company Name> when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of <Company Name>. Employees assume any and all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, <Company Name>’s trademarks, logos and any other <Company Name> intellectual property may also not be used in connection with any blogging activity

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term **Definition**

Blogging Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Spam Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History

This section is used to record version changes.

More Information

To find out more on the creation and testing of policy visit the following sites:

- The SANS Policy Website
    - http://www.sans.org/resources/policies/
    - The SANS Security Policy Resource page is a consensus research project of the SANS community. The ultimate goal of the project is to offer everything you need for rapid development and implementation of information security policies. You'll find a great set of resources posted here already including policy templates for twenty-four important security requirements.
- Information Security Policy - A Development Guide for Large and Small Companies
    - http://www.sans.org/reading_room/whitepapers/policyissues/1331.php
    - A security policy should fulfill many purposes. It should: protect people and information; set the rules for expected behavior by users, system administrators, management, and security personnel; authorize security personnel to monitor, probe, and investigate; define and authorize the consequences of violation; define the company consensus baseline stance on security; help minimize risk; and help track compliance with regulations and legislation.
- SANS Policy Primer
    - http://www.sans.org/resources/policies/Policy_Primer.pdf

    - This short primer on developing and writing security policies was taken from Michele D. Guel's full day tutorial titled "Security Governance – A Strong Foundation for a Secure Enterprise.

- RUsecure Information Security Policies
    - http://www.information-security-policies.com/
    - A commercial Policy creation program
- Technical Writing for IT Security Policies in Five Easy Steps
    - http://www.sans.org/reading_room/whitepapers/policyissues/492.php
    - As management requires more policies, staff comfort levels drop. As policy writers include complex, confusing, and incomprehensible language, staff comfort levels continue to drop. Therefore, IT Security policy writers need a writing resource, not just a policy resource. This paper points new policy technical writers in the right direction and provides a solid foundation from which to start. Follow these five easy steps when writing IT Security policies. Your management and employees will thank you.
- Security Policy Roadmap - Process for Creating Security Policies
    - http://www.sans.org/reading_room/whitepapers/policyissues/494.php
    - Information is an important business asset and is valuable to an organization. Thus, it needs to be protected to ensure its confidentiality, integrity and availability. The very first thing in information security is to set up policies and procedures on how to protect information. This paper presents a systematic approach in developing computer security policies and procedures. All the processes in the Policy Life Cycle will be discussed. In particular, it will list all the issues and factors that must be considered when setting up the policies. It makes some recommendations and suggestions on relevant areas and produces a framework for setting security policies and procedures
- SANS Score - Security Consensus Operational Readiness Evaluation
    - http://www.sans.org/score/
    - SCORE is a cooperative effort between SANS/GIAC and the Center for Internet Security(CIS). SCORE is a community of security professionals from a wide range of organizations and backgrounds working to develop consensus regarding minimum standards and best practice information, essentially acting as the research engine for CIS. After consensus is reached and best practice recommendations are validated, they may be formalized by CIS as best practice and minimum standards benchmarks for general use by industry at large.
    - SCORE Objectives:
        - Promote, develop and publish security checklists.

- Build these checklists via consensus, and through open discussion through SCORE mailing lists.
- Use existing references, recruit GIAC-certified professionals, and enlist subject matter experts, where and when possible.

These are but a few of the many places where information and frameworks are available that can be used in the creation of an information security policy program.

Summary

The security manager must seek first to understand when creating policy. Understand how the stakeholders would view the policy; understand the tradeoffs; understand the impact on people under the scope of the policy and avoid "policy tax", if at all possible; and, finally, understand what is going on in the reader's mind when they read the policy, how do they perceive it? Better policy is worth the effort - people cannot follow a policy if they cannot understand what it says.

Security policy needs to fulfill several purposes. It needs to:

- Protect people and information;
- Set the rules for expected behavior by employees and other users, system administrators, management, and security personnel;
- Provides authorization that enables security personnel to monitor, probe, and investigate incidents;
- Defines and authorizes actions associated with the consequences of a violation;
- Defines the organizational consensus baseline stance on security and helps make staff aware of the views of the organization and senior management; and
- Aids in creating an environment that minimizes risk; and
- Aids in remaining compliant to the regulations and legislation that applies to the organization.