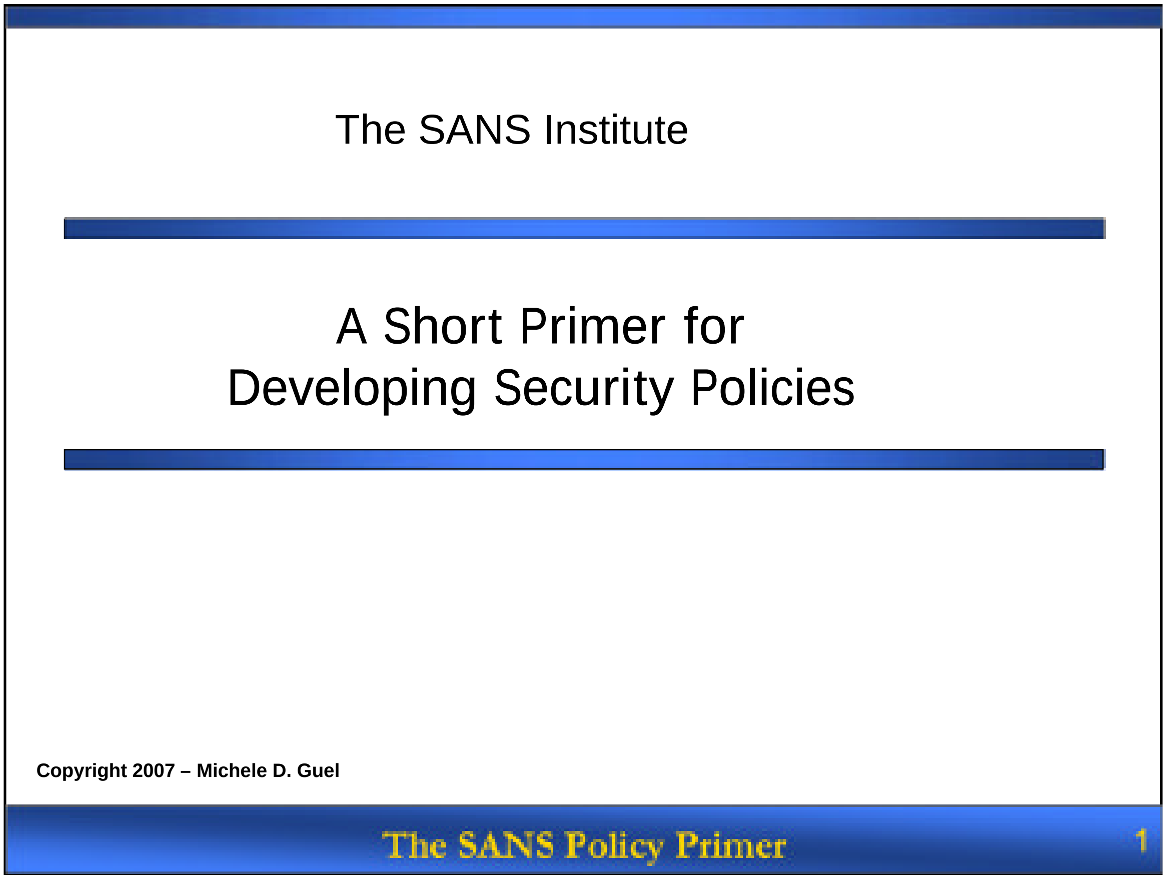
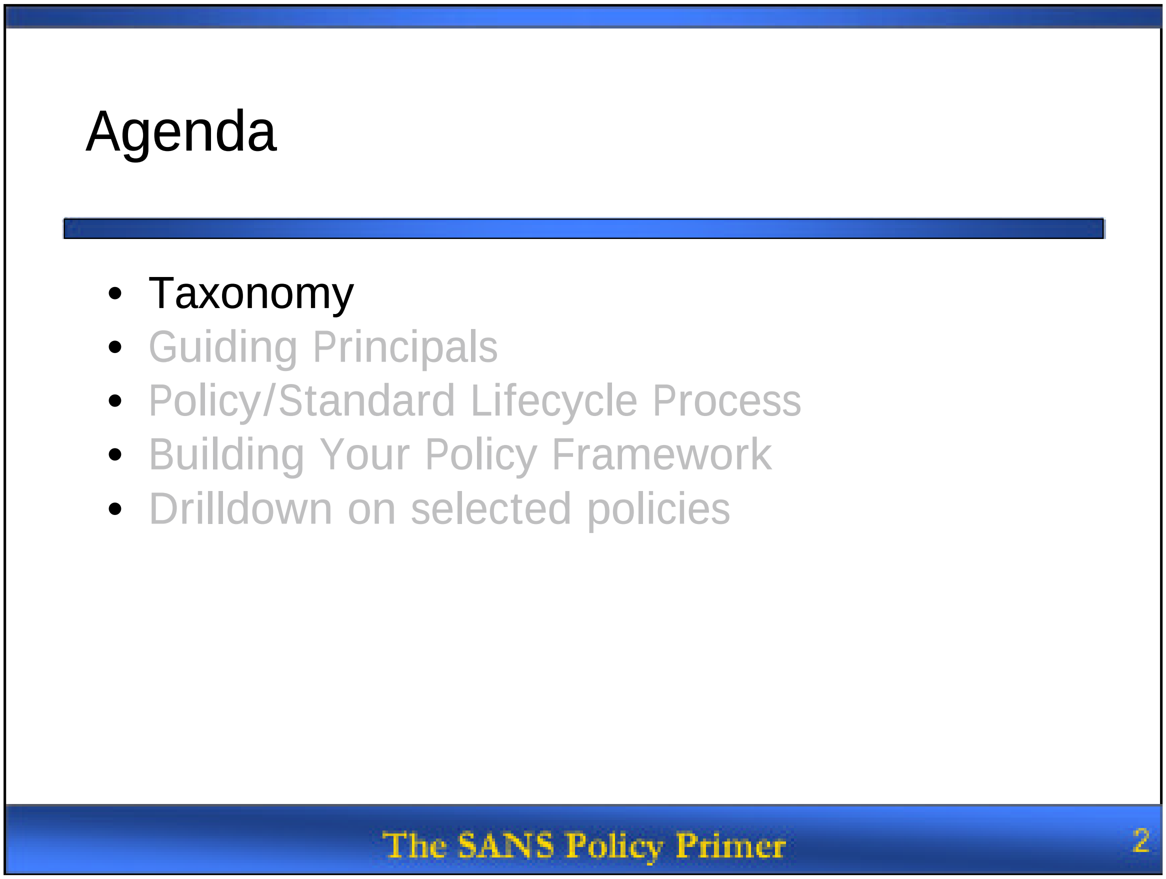


The SANS Institute

A Short Primer for Developing Security Policies

The SANS Policy Primer 1

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. Some materials were taken (with permission) from work done by Dave Vander Meer at Cisco Systems, Inc.

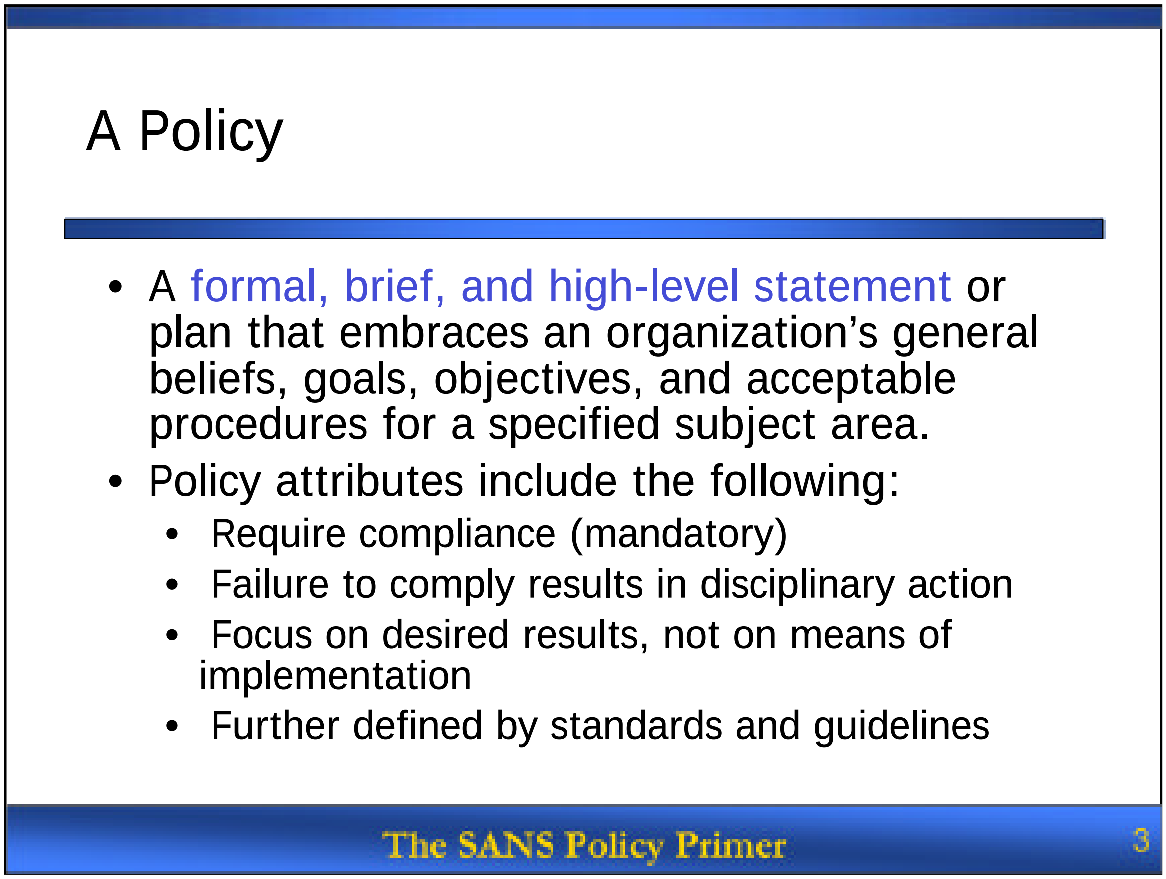


Agenda

- Taxonomy
- Guiding Principals
- Policy/Standard Lifecycle Process
- Building Your Policy Framework
- Drilldown on selected policies

The SANS Policy Primer 2

In this first section we are going to look at the taxonomy for various terms such as policy, standard, guideline, procedure and policy impact assessment. It is important to define and use these terms consistently within an organization.

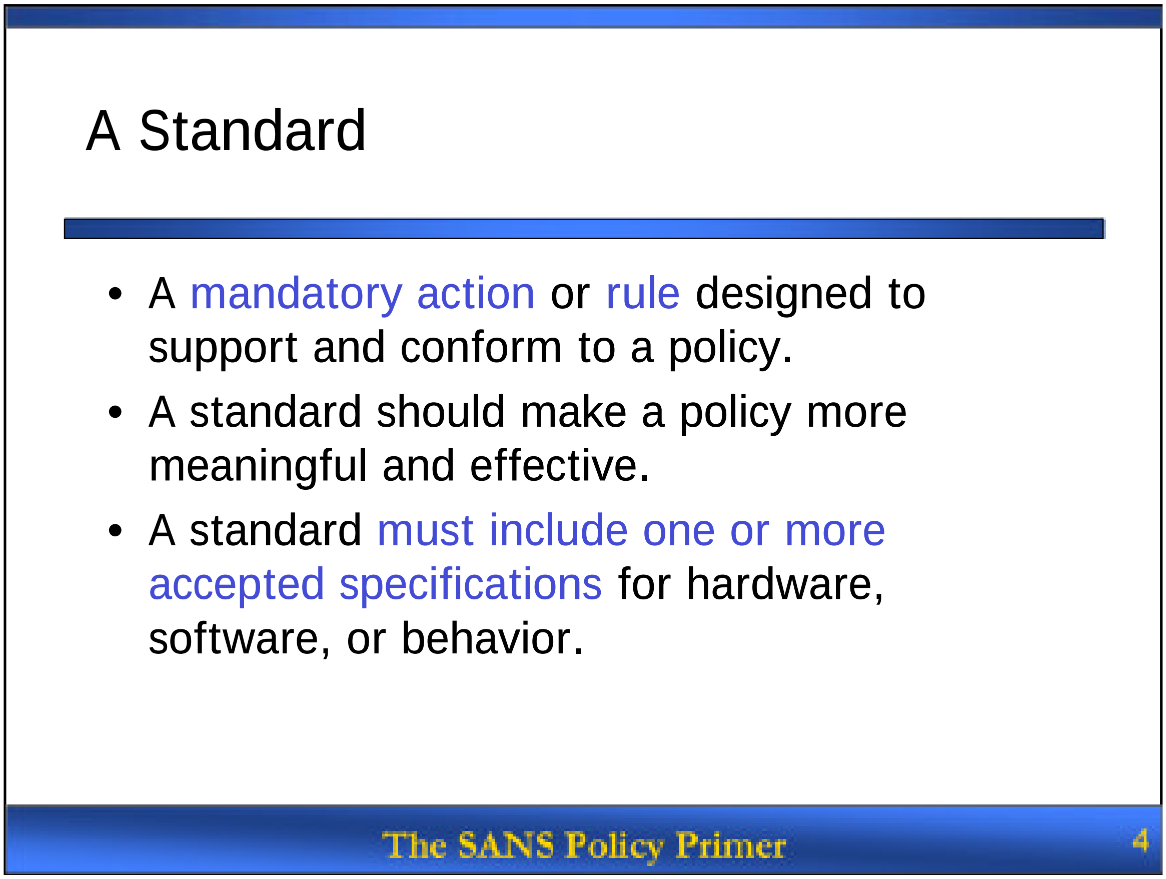


A Policy

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

The SANS Policy Primer 3

Policies always state required actions, and may include pointers to standards. Policies for a specific part of the organization should also include the same sections or element such as overview, scope, policy statements, enforcement and definitions. A policy template is discussed on pages 35-37.

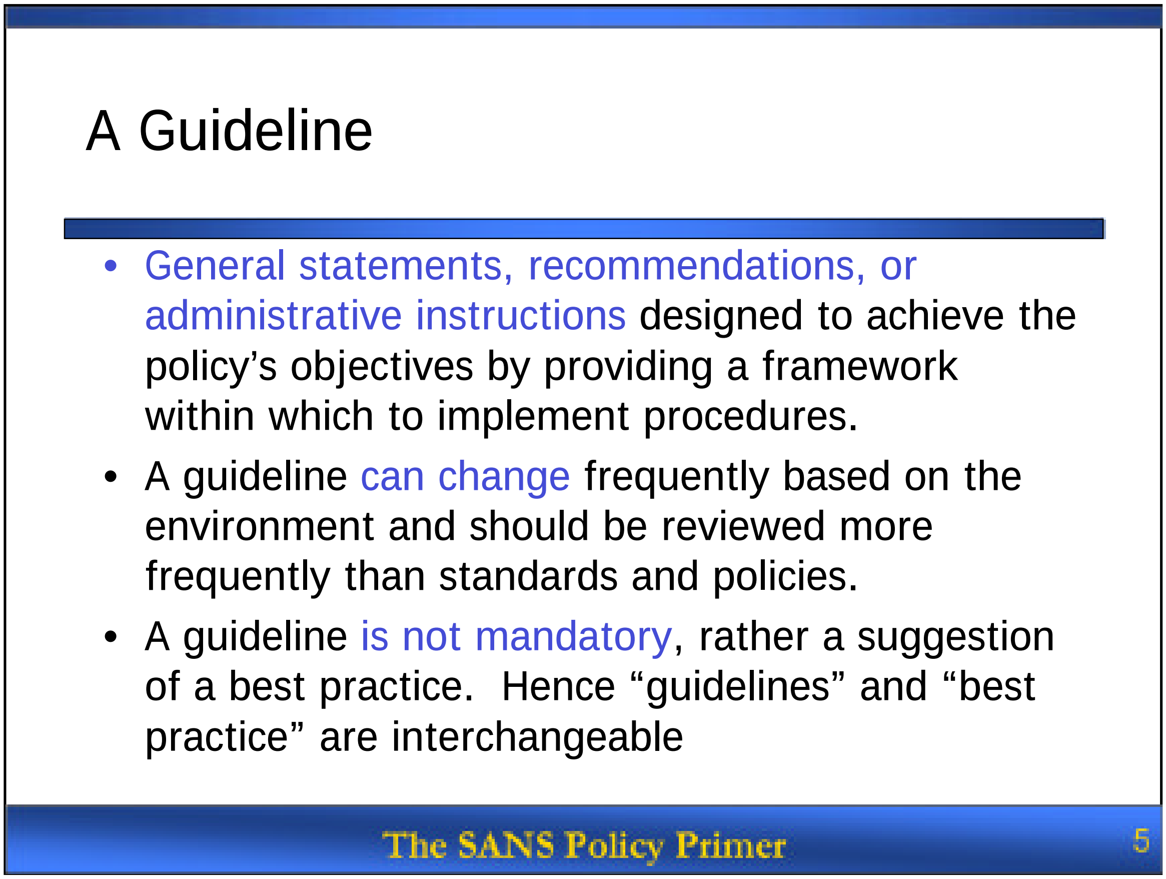


A Standard

- A mandatory action or rule designed to support and conform to a policy.
- A standard should make a policy more meaningful and effective.
- A standard must include one or more accepted specifications for hardware, software, or behavior.

The SANS Policy Primer 4

Standards are usually written to describe the requirements for various technology configurations (e.g., wireless set-up, harden an O/S or router). A standard is meant to convey a mandatory action or rule and is written in conjunction with a policy. For example, many organizations should (and need) to have a policy about the use of wireless technology. The wireless policy should have an accompanying wireless standard which discusses the specific protocols that are required, encryption key requirements, and specific configuration setup for the production network as well as home networks.

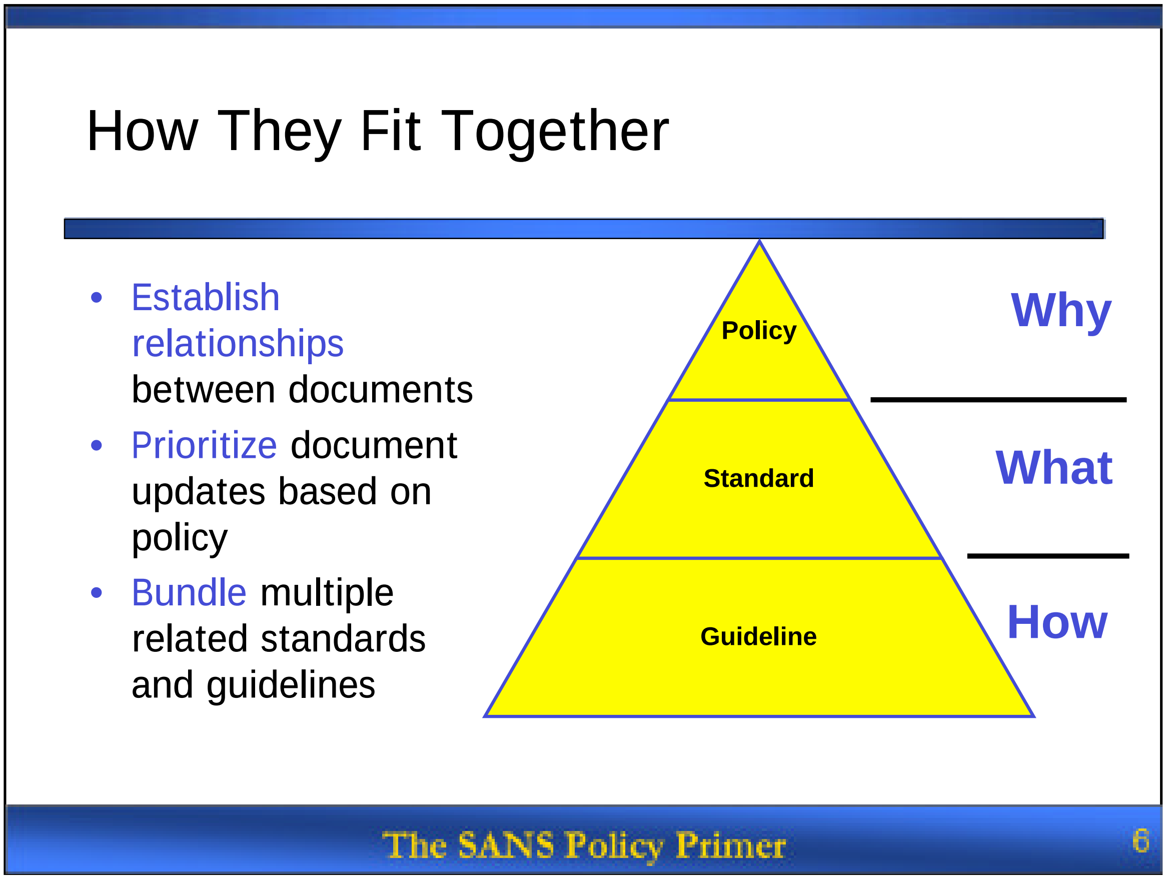


A Guideline

- General statements, recommendations, or administrative instructions designed to achieve the policy’s objectives by providing a framework within which to implement procedures.
- A guideline can change frequently based on the environment and should be reviewed more frequently than standards and policies.
- A guideline is not mandatory, rather a suggestion of a best practice. Hence “guidelines” and “best practice” are interchangeable

The SANS Policy Primer 5

Guidelines are not a required element of a policy framework; however, they can play an important role in conveying best practice information to the user community. Guidelines are meant to “guide” users to adopt behaviors which increase the security posture of a network, but are not yet required (or in some cases, my never be required). For example, an organization might choose to publish a guideline on how to secure home networks even though they are not supported by the corporation. Guidelines can also be used as a pre-cursor for what will eventually become a policy issue.

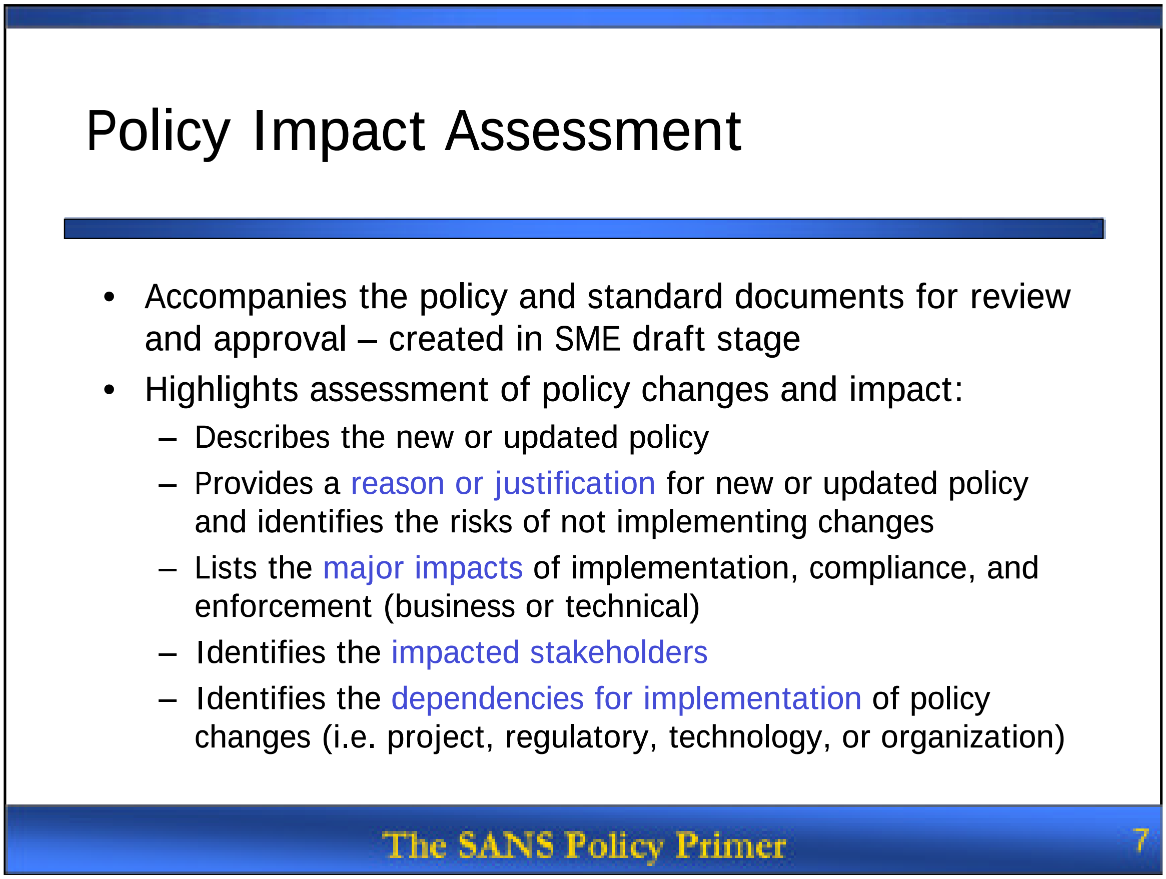


How They Fit Together

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

The SANS Policy Primer 6

The diagram demonstrates the relationship between guidelines, standards and policies. Guidelines describe best practices on how to do something, say harden a MS Vista box for the DMZ. Standards describe what the baseline requirements are for various technologies and configurations that are supported in the enterprise. Policies describe required actions to take and why.

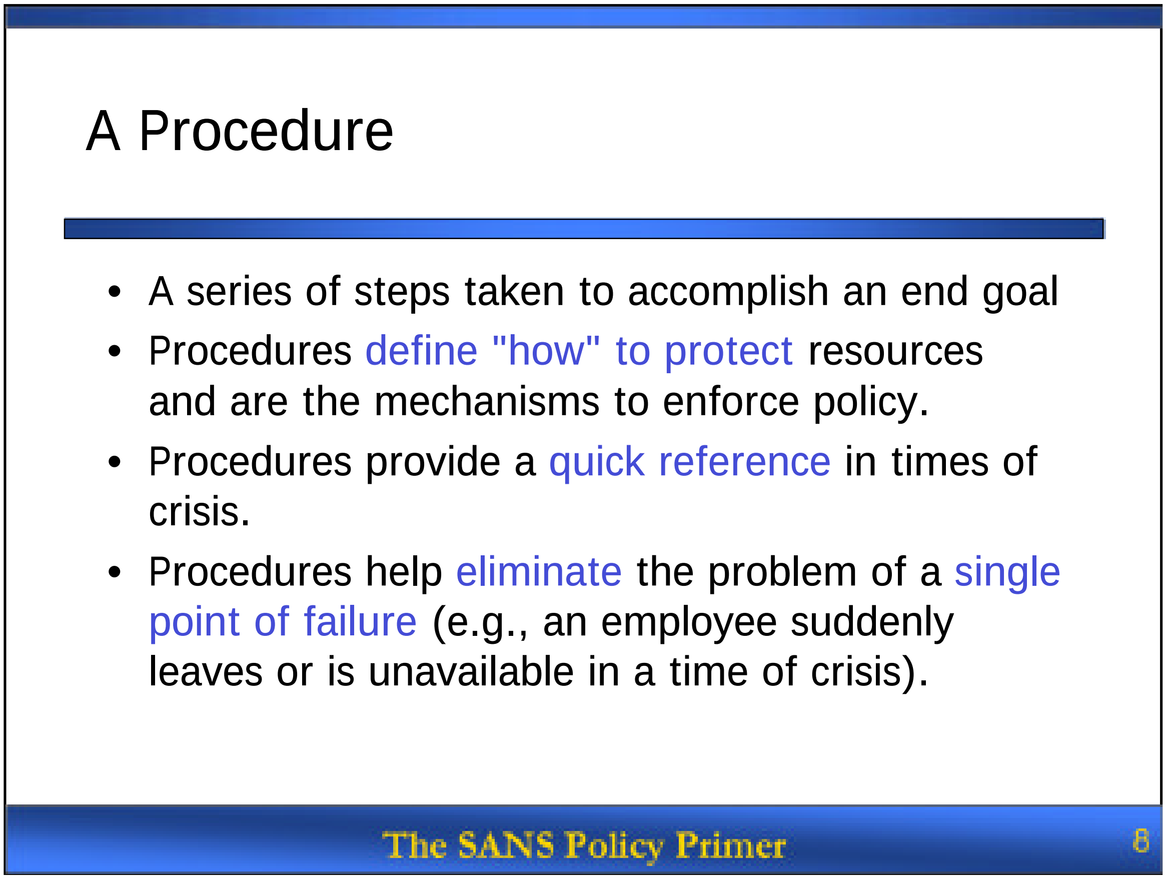


Policy Impact Assessment

- Accompanies the policy and standard documents for review and approval – created in SME draft stage
- Highlights assessment of policy changes and impact:
  - Describes the new or updated policy
  - Provides a reason or justification for new or updated policy and identifies the risks of not implementing changes
  - Lists the major impacts of implementation, compliance, and enforcement (business or technical)
  - Identifies the impacted stakeholders
  - Identifies the dependencies for implementation of policy changes (i.e. project, regulatory, technology, or organization)

The SANS Policy Primer 7

The policy impact assessment provides a quick overview of the changes made to the policy and how they will effect the enterprise, or what actions people will need to take to be compliant with the policy. The policy impact assessment also provides the reason or justification for the policy updates or new policy. In some cases, managers may only review the policy impact assessment rather than the actual policy.

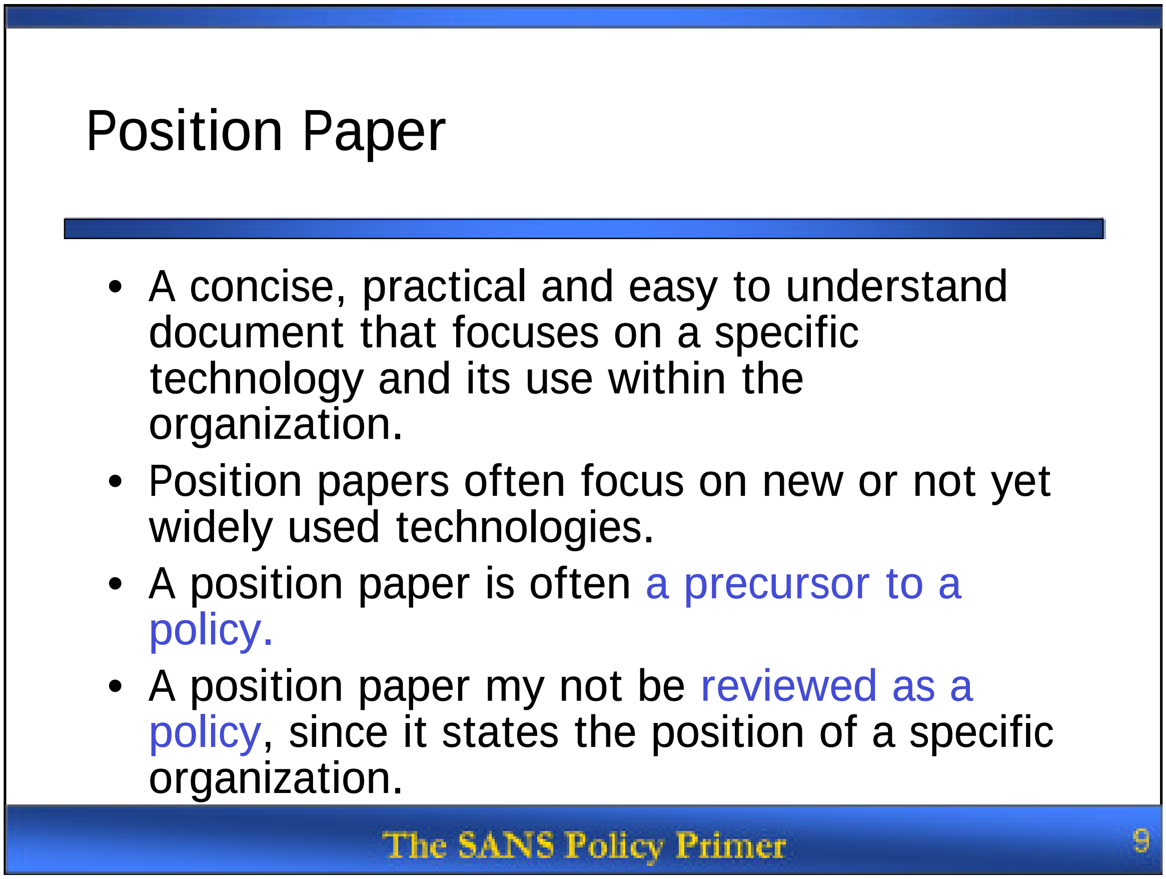


A Procedure

- A series of steps taken to accomplish an end goal
- Procedures define "how" to protect resources and are the mechanisms to enforce policy.
- Procedures provide a quick reference in times of crisis.
- Procedures help eliminate the problem of a single point of failure (e.g., an employee suddenly leaves or is unavailable in a time of crisis).

The SANS Policy Primer 8

Procedures are equally important as policies. Often the polices define what is to be protected and what are the ground rules. The procedures outline how to protect the resources or how to carry out the policies. For example, a Password Policy would outline password construction rules, rules on how to protect your password and how often to change them. The Password Management Procedure would outline the process to create new passwords, distribute them as well as the process for ensuring the passwords have changed on critical devices. There will not always be a one-to-one relationship between policy and procedures.

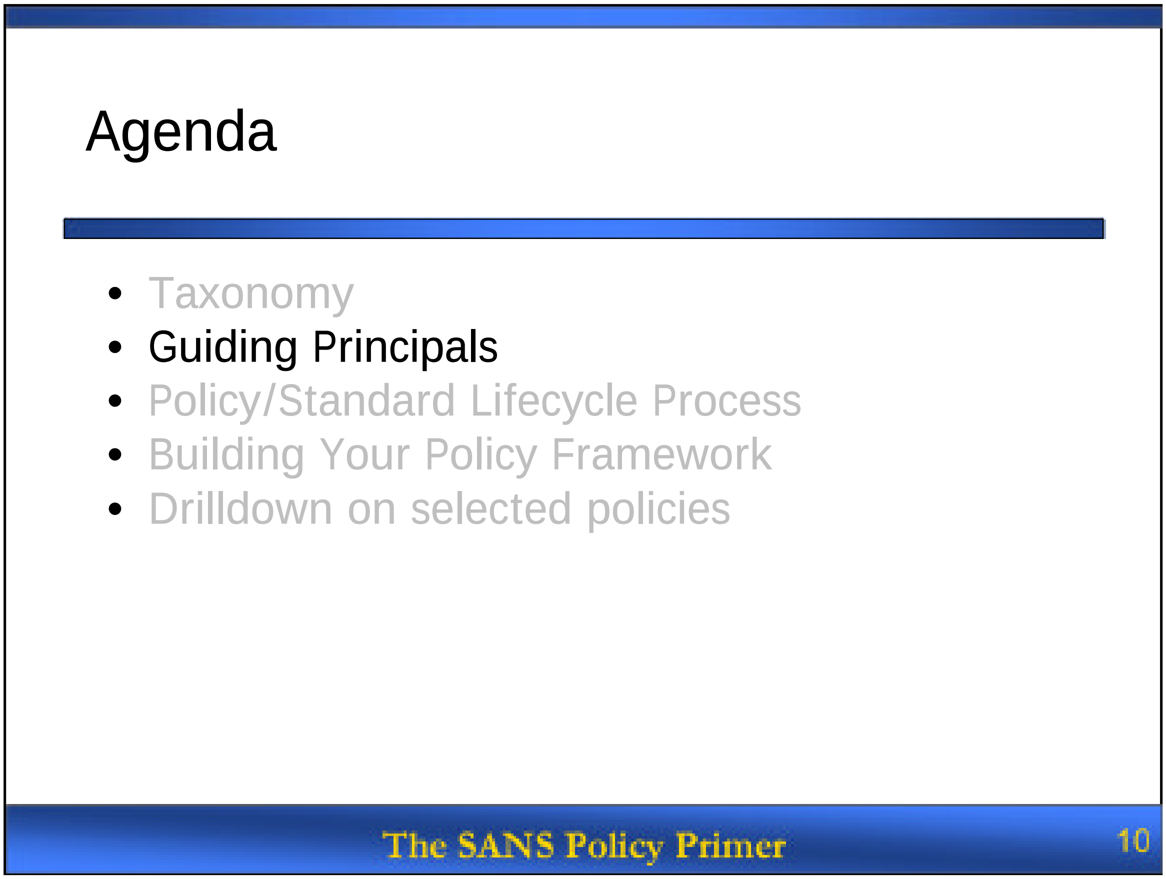


Position Paper

- A concise, practical and easy to understand document that focuses on a specific technology and its use within the organization.
- Position papers often focus on new or not yet widely used technologies.
- A position paper is often a precursor to a policy.
- A position paper my not be reviewed as a policy, since it states the position of a specific organization.

The SANS Policy Primer 9

A position paper can be an effective way to socialize a security organizations initial views and concerns around new technology. Often, users will begin to experiment and use new technologies long before an organization may adopt and officially support them. Or in some cases, an organization may never support certain technologies, but would like to provide guidance to their user base concerning specific technologies. Position papers can also fill a gap where there are gray areas such that a policy or standard is not appropriate.

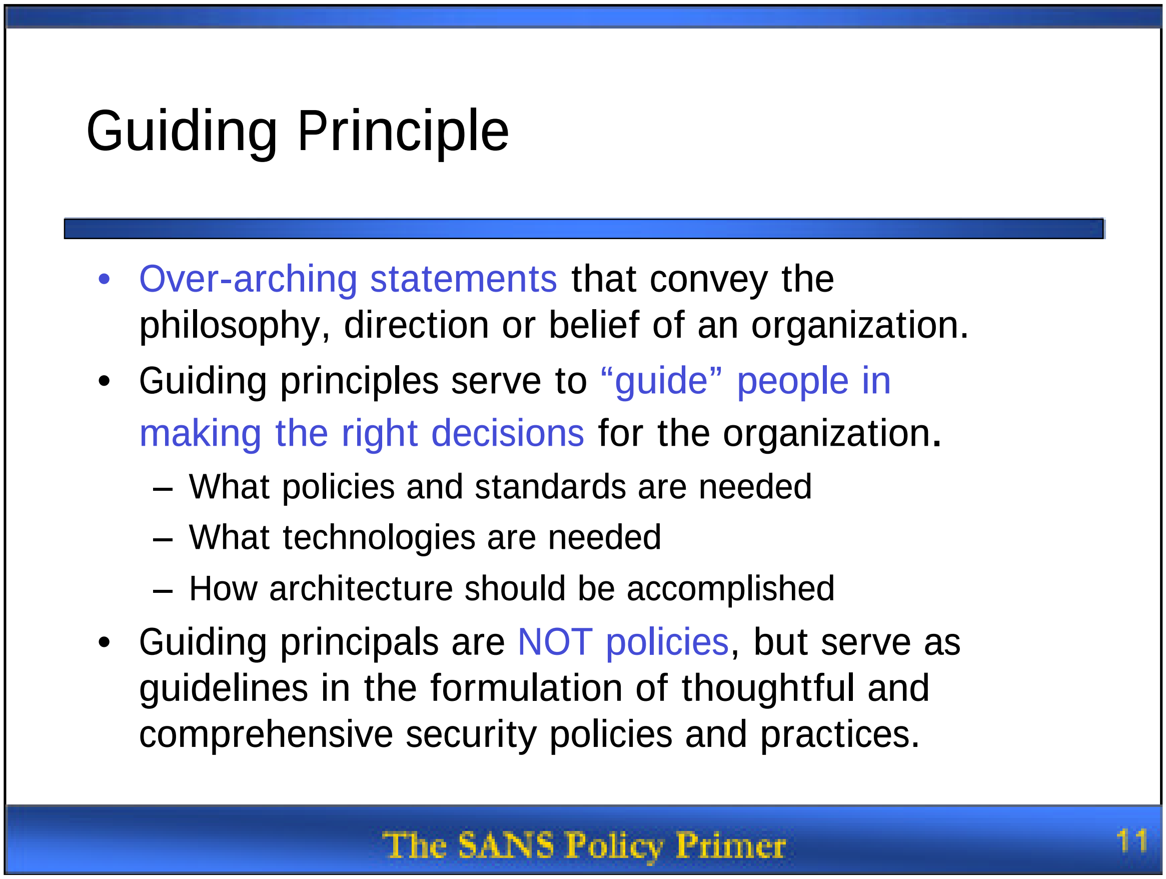


Agenda

- Taxonomy
- Guiding Principals
- Policy/Standard Lifecycle Process
- Building Your Policy Framework
- Drilldown on selected policies

The SANS Policy Primer 10

In this section we will cover guiding principles. We will define what a guiding principle is, why they are needed, and provide some examples of actual guiding principles in use at organizations.

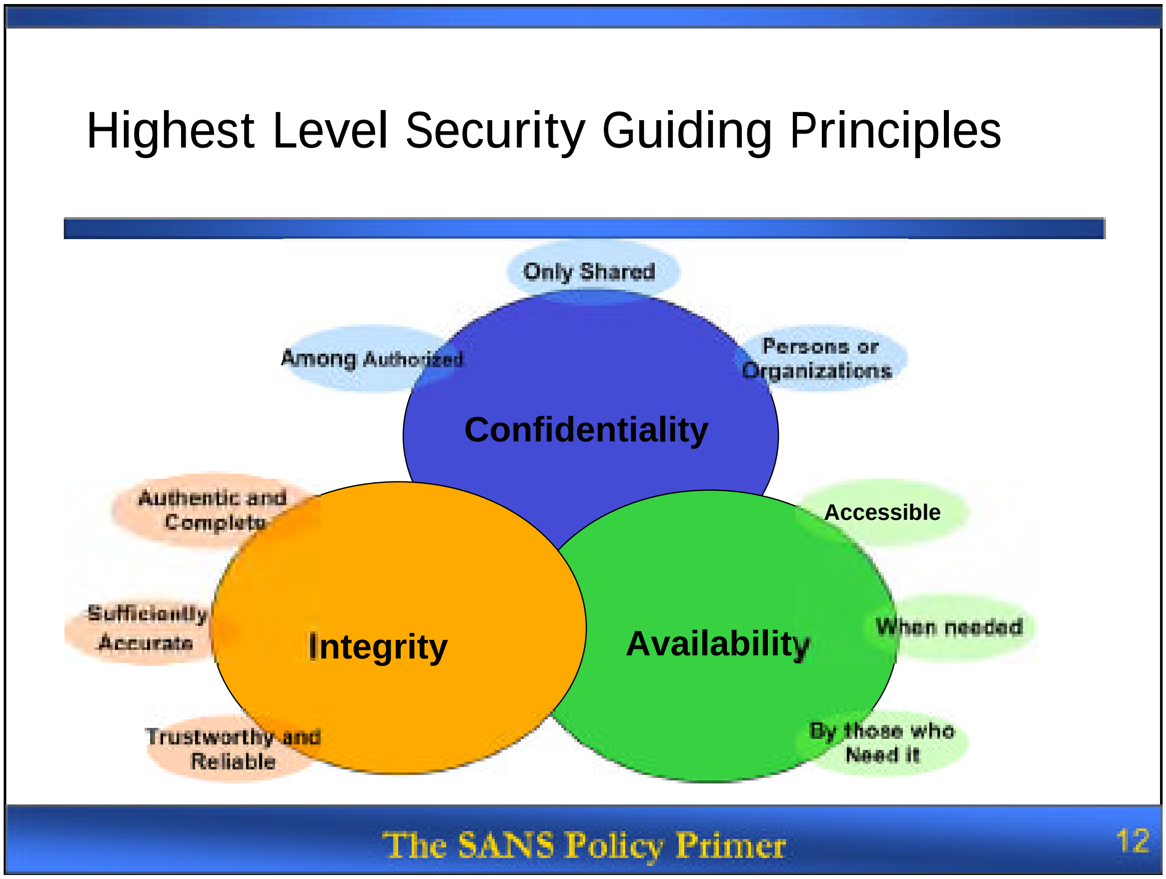


Guiding Principle

- Over-arching statements that convey the philosophy, direction or belief of an organization.
- Guiding principles serve to “guide” people in making the right decisions for the organization.
  - What policies and standards are needed
  - What technologies are needed
  - How architecture should be accomplished
- Guiding principals are NOT policies, but serve as guidelines in the formulation of thoughtful and comprehensive security policies and practices.

The SANS Policy Primer 11

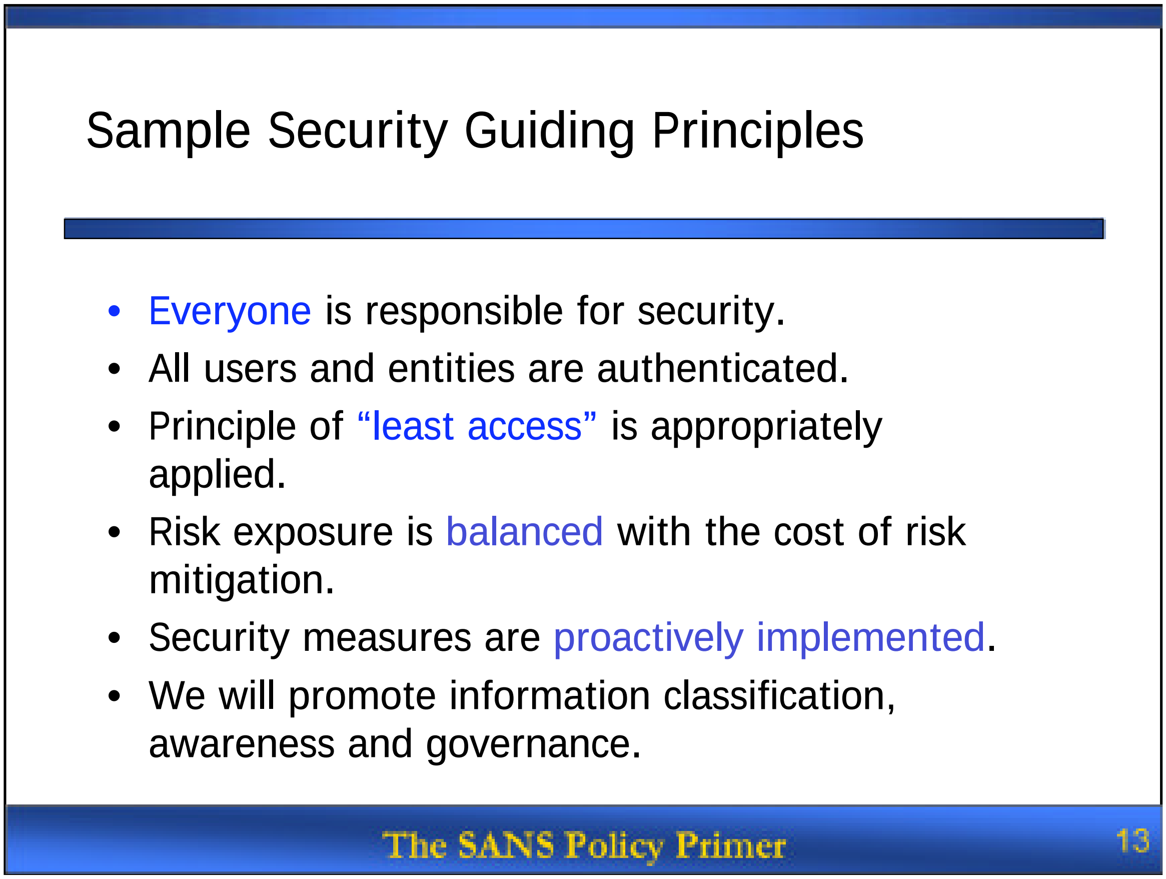
Guiding principles are over-arching statements that convey the direction or belief of an organization. They server to “guide” people in making the right decisions (such a technology purchases or architecture direction). They can also serve as a guide-post on what policies and standards will be needed by an organization. Guiding principles provide a strong foundation for any organization. They can be specific to a certain function (e.g. Corporate Security) or more general such as IT Guiding Principles.



Highest Level Security Guiding Principles

The SANS Policy Primer 12

Every security organization should be concerned about the integrity, confidentiality and availability of their key information assets and resources and this should be reflected in one or more of their key security guiding principals.

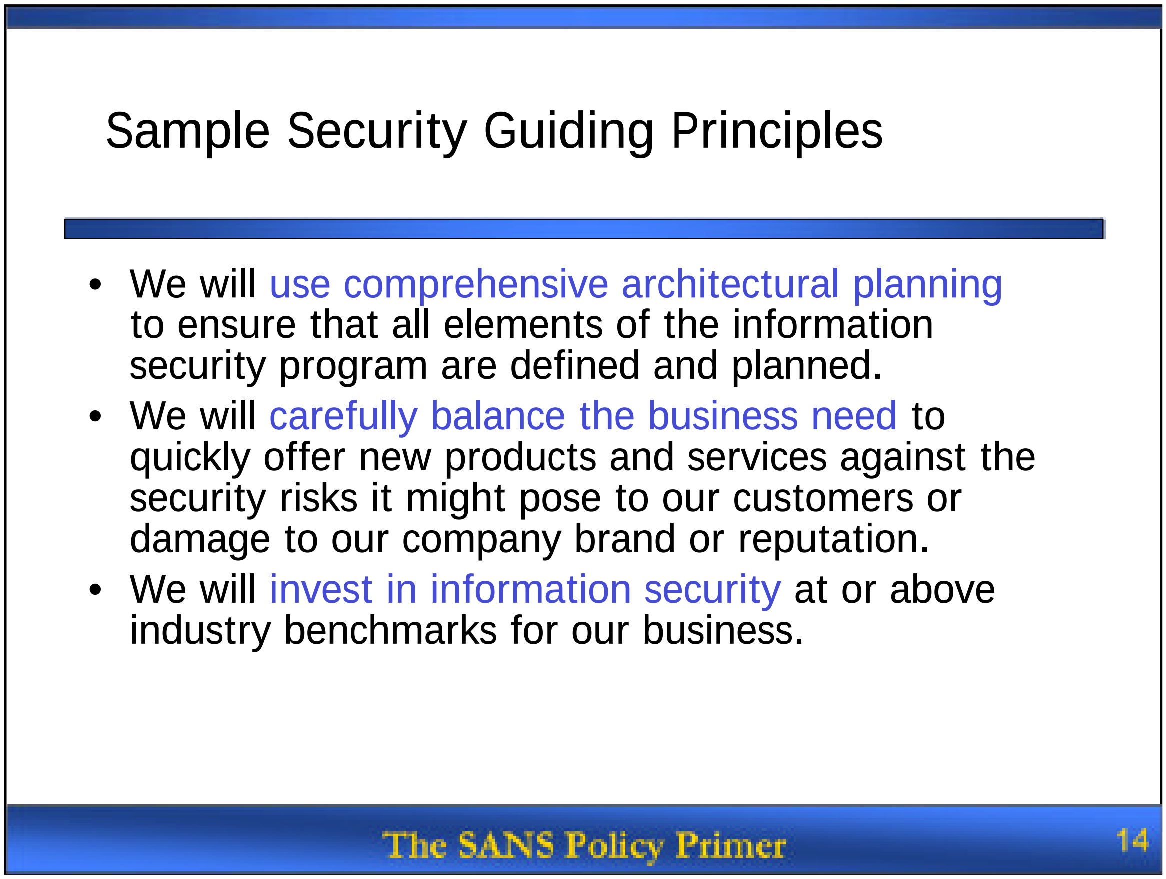


Sample Security Guiding Principles

- Everyone is responsible for security.
- All users and entities are authenticated.
- Principle of “least access” is appropriately applied.
- Risk exposure is balanced with the cost of risk mitigation.
- Security measures are proactively implemented.
- We will promote information classification, awareness and governance.

The SANS Policy Primer 13

These are examples of actual guiding principles used in various organizations. Some of the statements are very short and to the point. Take the first statement – everyone is responsible for security. This principle lets all users in an organization know they are expected to play a role in securing the organization through their personal behavior. The statement about Risk exposure being balanced with the cost of risk mitigation, demonstrates that an organization carefully considers the cost impact of proposed mitigation efforts.

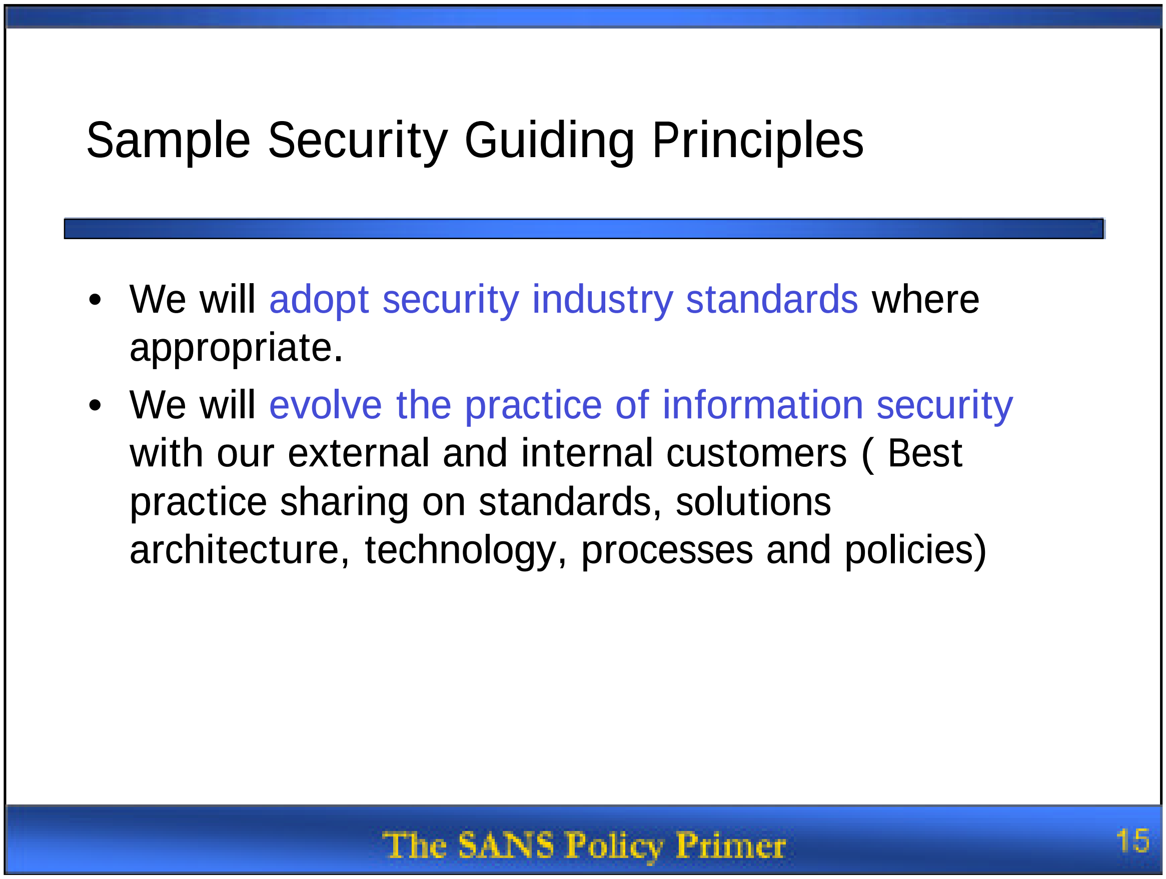


Sample Security Guiding Principles

- We will use comprehensive architectural planning to ensure that all elements of the information security program are defined and planned.
- We will carefully balance the business need to quickly offer new products and services against the security risks it might pose to our customers or damage to our company brand or reputation.
- We will invest in information security at or above industry benchmarks for our business.

The SANS Policy Primer 14

The example guiding principals on this page will guide an organization about choices they make with respect to implementing new technologies or making architectural decisions.   The last bullet would guide an organization on decisions they make with respect to budgeting for the security function.

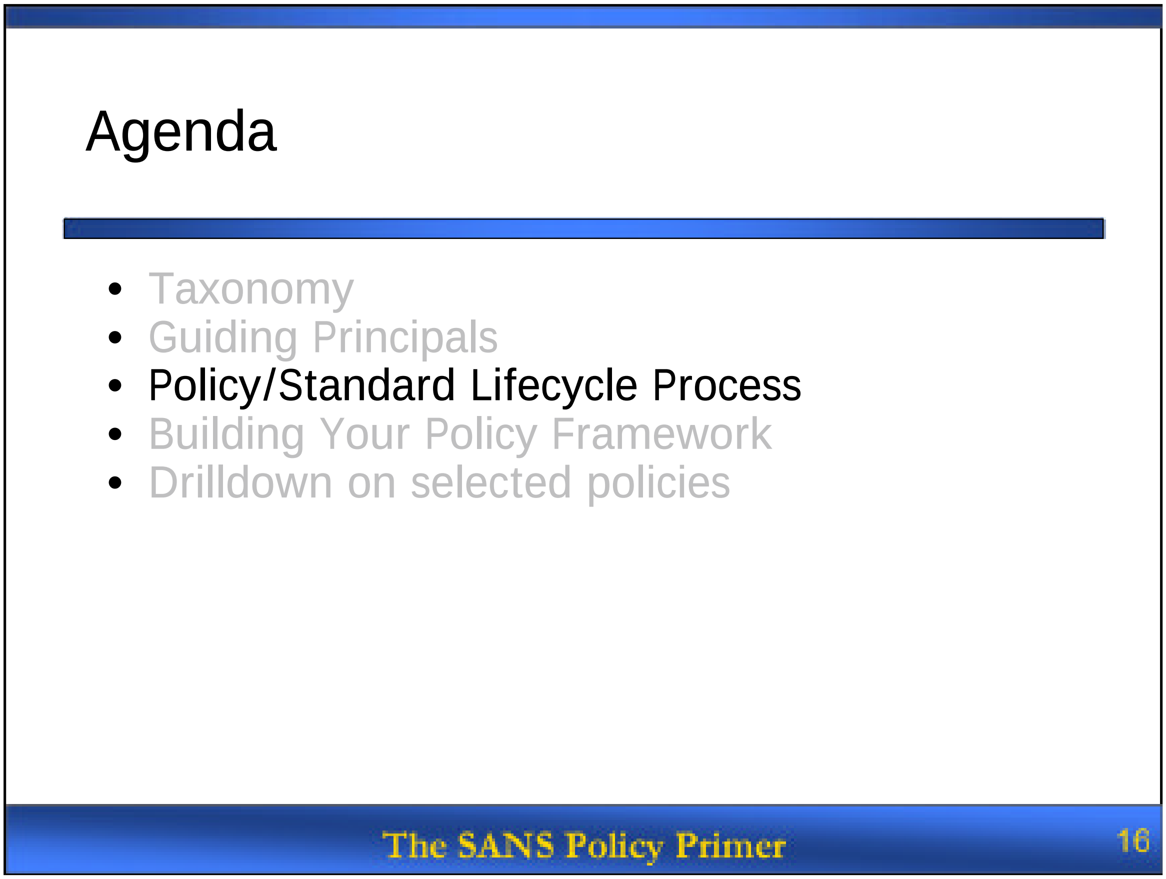


Sample Security Guiding Principles

- We will adopt security industry standards where appropriate.
- We will evolve the practice of information security with our external and internal customers (Best practice sharing on standards, solutions architecture, technology, processes and policies)

The SANS Policy Primer 15

More examples of guiding principles. The first bullet speaks to the fact that this organization is committed to adopting industry standards where appropriate. Following industry standards is often a good direction and practice for an organization. The second bullet speaks to the fact that this organization considers sharing best practices with external organization a key a function in their overall purpose.

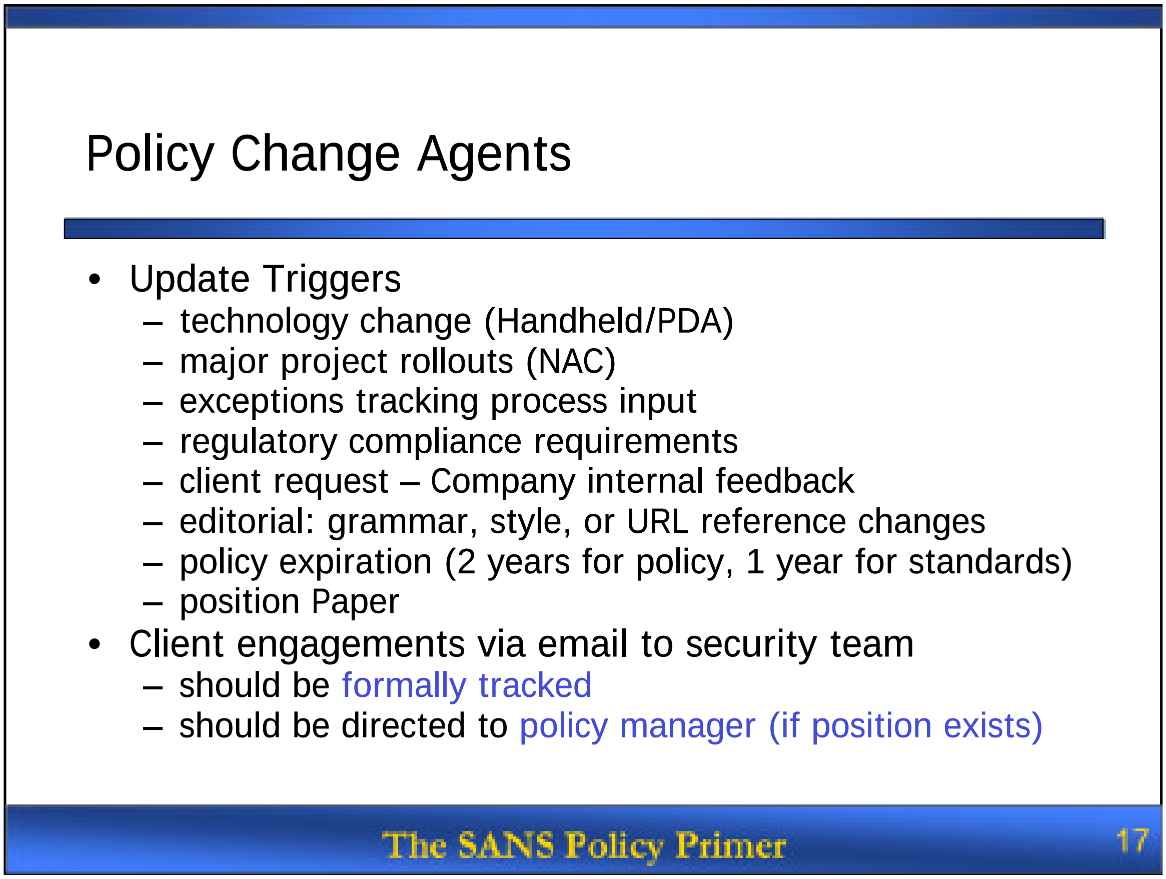


Agenda

- Taxonomy
- Guiding Principals
- Policy/Standard Lifecycle Process
- Building Your Policy Framework
- Drilldown on selected policies

The SANS Policy Primer 16

In this section we are going to example the Policy Lifecycle process. We will discuss some common policy change agents and then we will look at the lifecycle process in-depth.



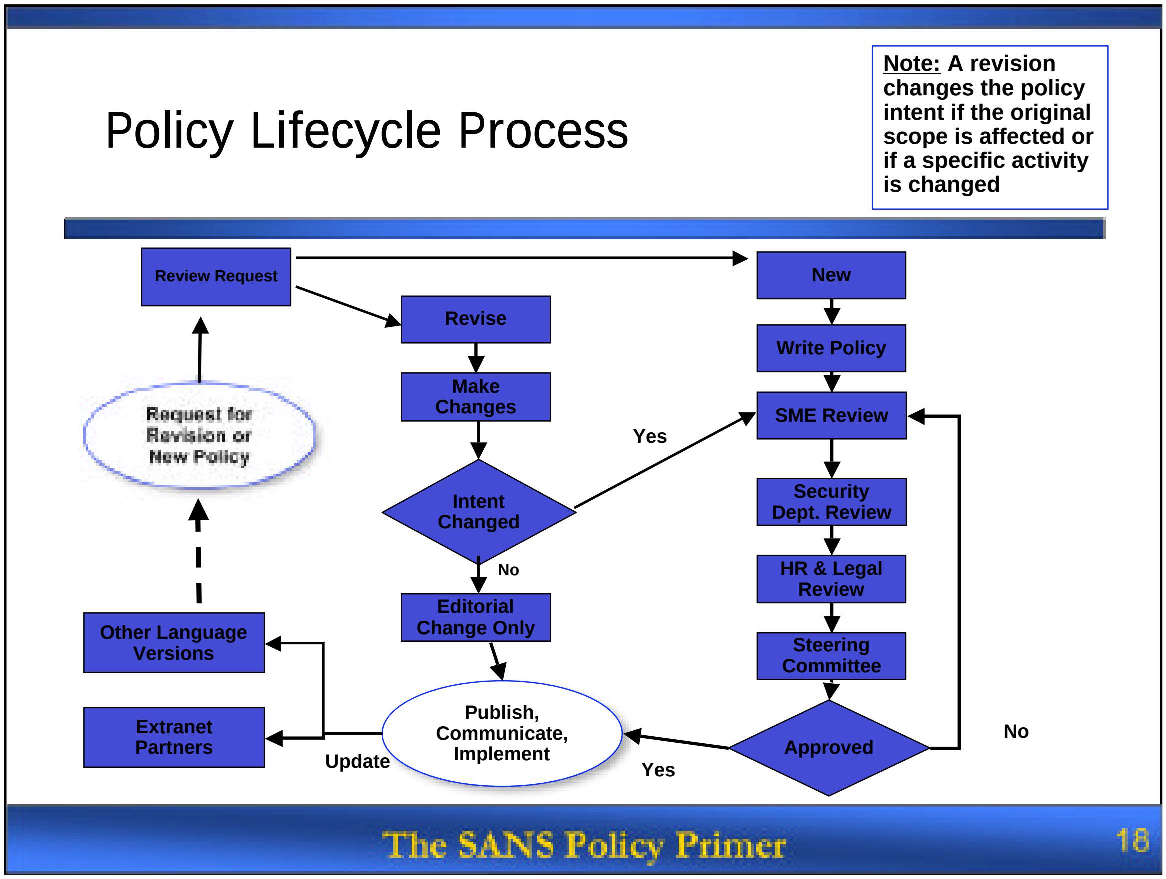
Policy Change Agents

- Update Triggers
  - technology change (Handheld/PDA)
  - major project rollouts (NAC)
  - exceptions tracking process input
  - regulatory compliance requirements
  - client request – Company internal feedback
  - editorial: grammar, style, or URL reference changes
  - policy expiration (2 years for policy, 1 year for standards)
  - position Paper
- Client engagements via email to security team
  - should be formally tracked
  - should be directed to policy manager (if position exists)

The SANS Policy Primer 17

There are various events that can trigger the need to review and update a policy. New technology rollouts are one key event which usually triggers the need for a new policy and updates to existing policies. State or federal regulatory compliance requirements will almost always necessitate review and update of existing policies, as well as the need for new policies. Sometimes user's behavior to existing policies will trigger a need to review that policy for potential changes.

It is recommended that organizations track correspondences regarding requests for changes to existing policies or a request for a new policy. In some cases, such tracking might be required to meet SoX compliance.



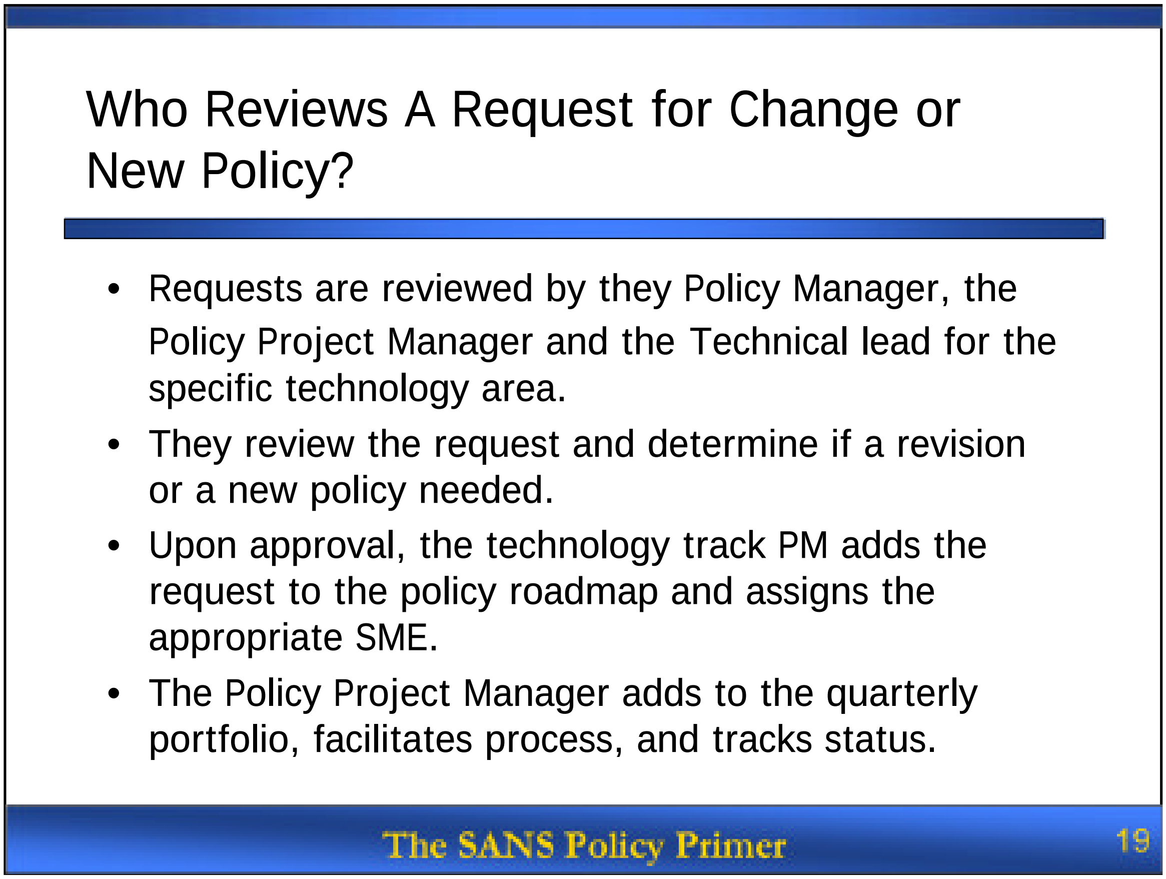
Policy Lifecycle Process

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

The SANS Policy Primer 18

This diagram depicts an example of a policy lifecycle process. On the left top corner we start with the policy review and request process. This will either trigger 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 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.

We’ll discuss each of the steps in detail on the following slides.



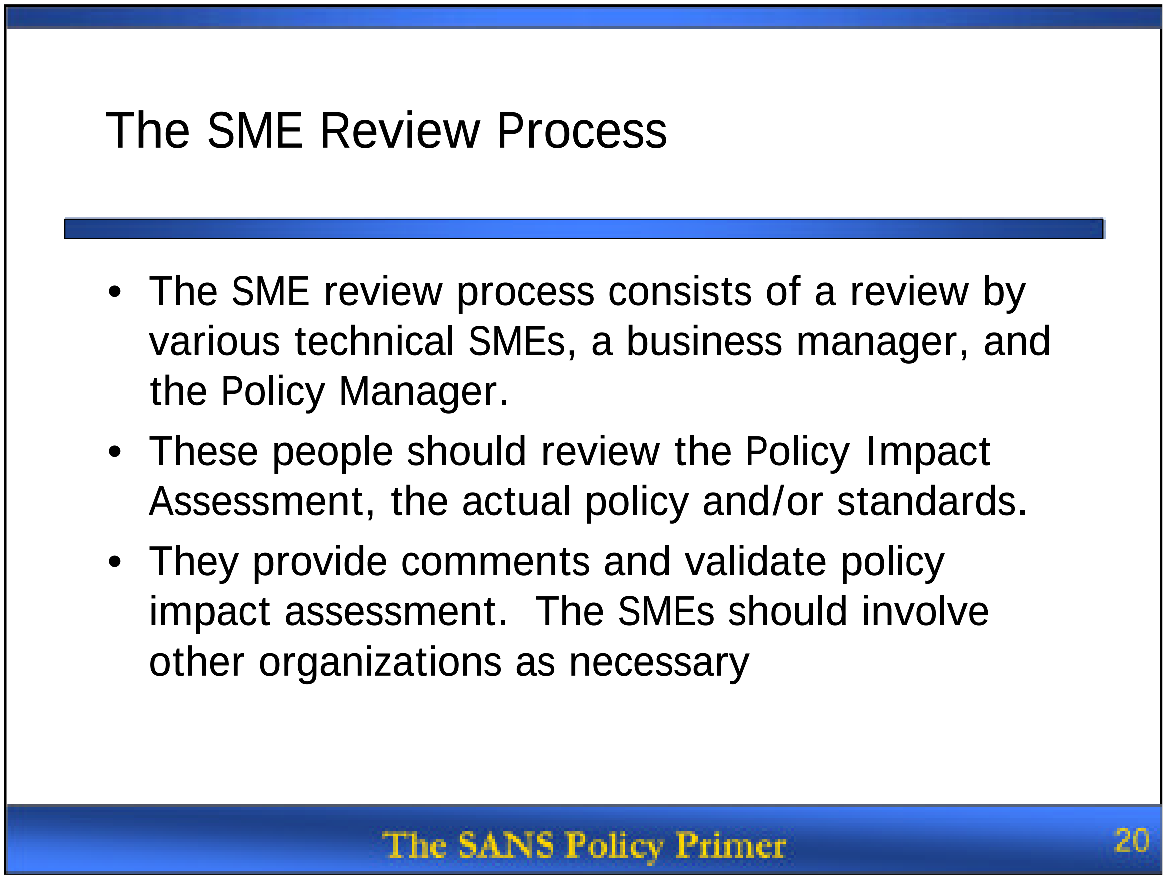
Who Reviews A Request for Change or New Policy?

- Requests are reviewed by they Policy Manager, the Policy Project Manager and the Technical lead for the specific technology area.
- They review the request and determine if a revision or a new policy needed.
- Upon approval, the technology track PM adds the request to the policy roadmap and assigns the appropriate SME.
- The Policy Project Manager adds to the quarterly portfolio, facilitates process, and tracks status.

The SANS Policy Primer 19

Large organizations with a lot of security policies should establish a periodic policy review process (perhaps quarterly or twice a year). The Policy Manager is the person who can make the call about the need or not for a new policy or update to an existing policy. This is usually a lead technical person within the organization. The Policy Project Manager is a PM (typically responsible for several areas) who manages the overall policy pipeline (from request to publication).

Most large organization will have ongoing policy activity – reviews, updates, new policies, standards, guidelines. This is very critical work for the organization and must be part of the overall portfolio process to ensure proper resources and budgeting.

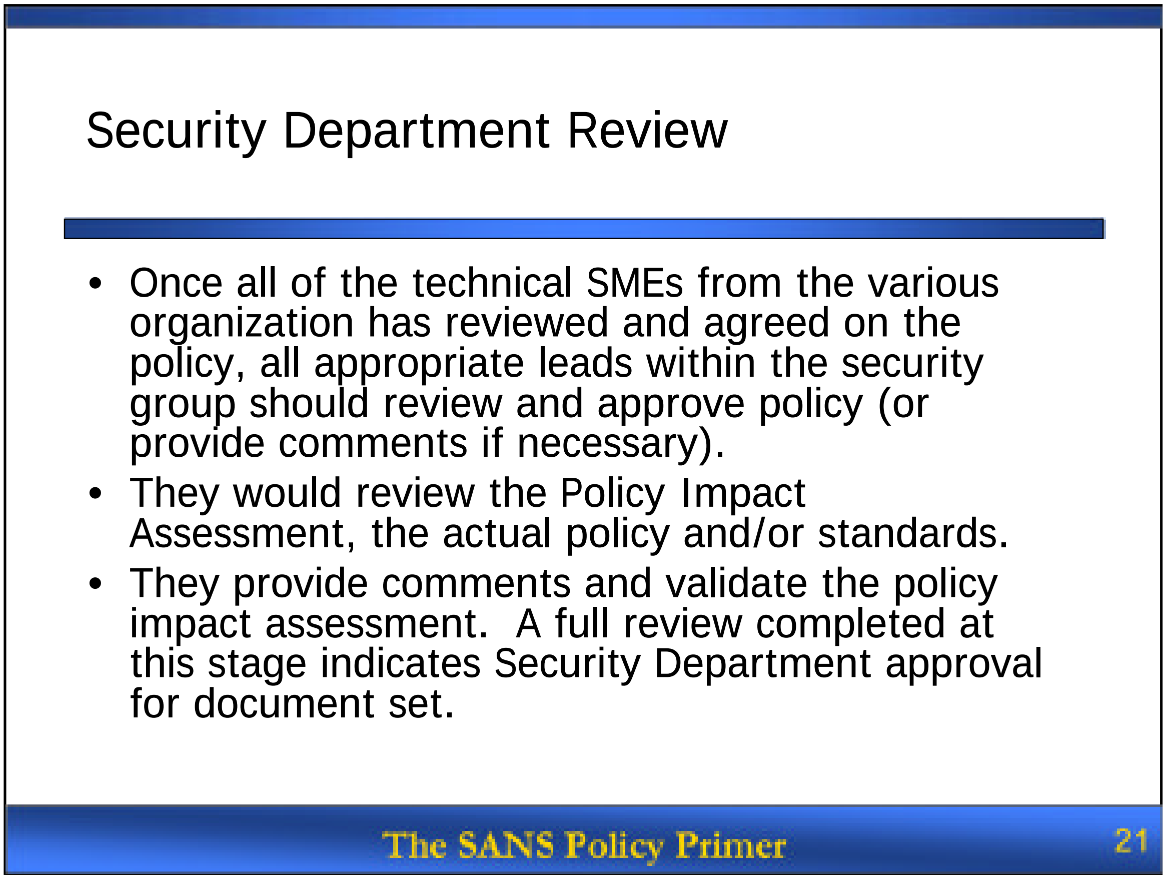


The SME Review Process

- The SME review process consists of a review by various technical SMEs, a business manager, and the Policy Manager.
- These people should review the Policy Impact Assessment, the actual policy and/or standards.
- They provide comments and validate policy impact assessment. The SMEs should involve other organizations as necessary

The SANS Policy Primer 20

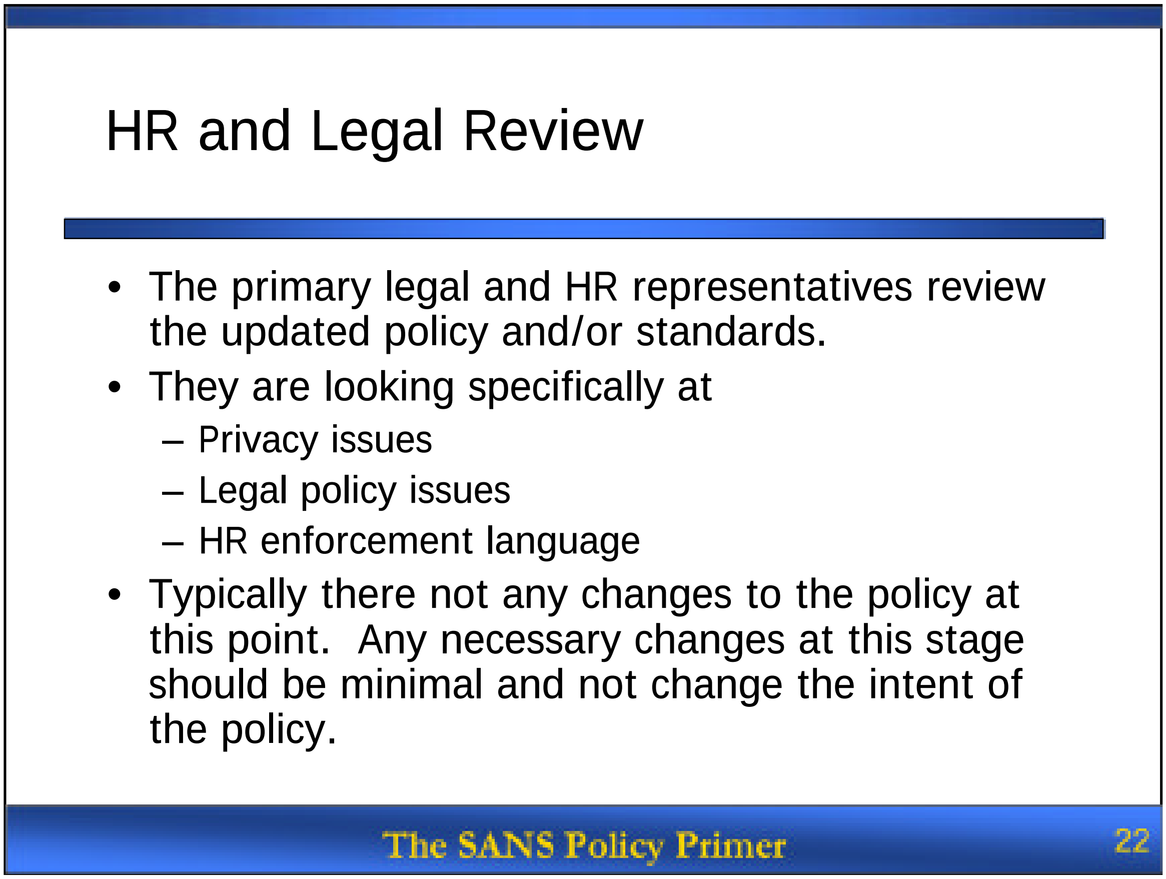
Every policy should have one or more assigned Subject Matter Experts who are familiar with the technology area of the policy (e.g. wireless). The policy SMEs are responsible for the initial review and update process.   Other departments and organizations should be involved as needed. The policy SME should provide guidance on who would be appropriate to review the policy. The Policy SME is also responsible for ensuring the accuracy of the Policy Impact Assessment.



Security Department Review

- Once all of the technical SMEs from the various organization has reviewed and agreed on the policy, all appropriate leads within the security group should review and approve policy (or provide comments if necessary).
- They would review the Policy Impact Assessment, the actual policy and/or standards.
- They provide comments and validate the policy impact assessment. A full review completed at this stage indicates Security Department approval for document set.

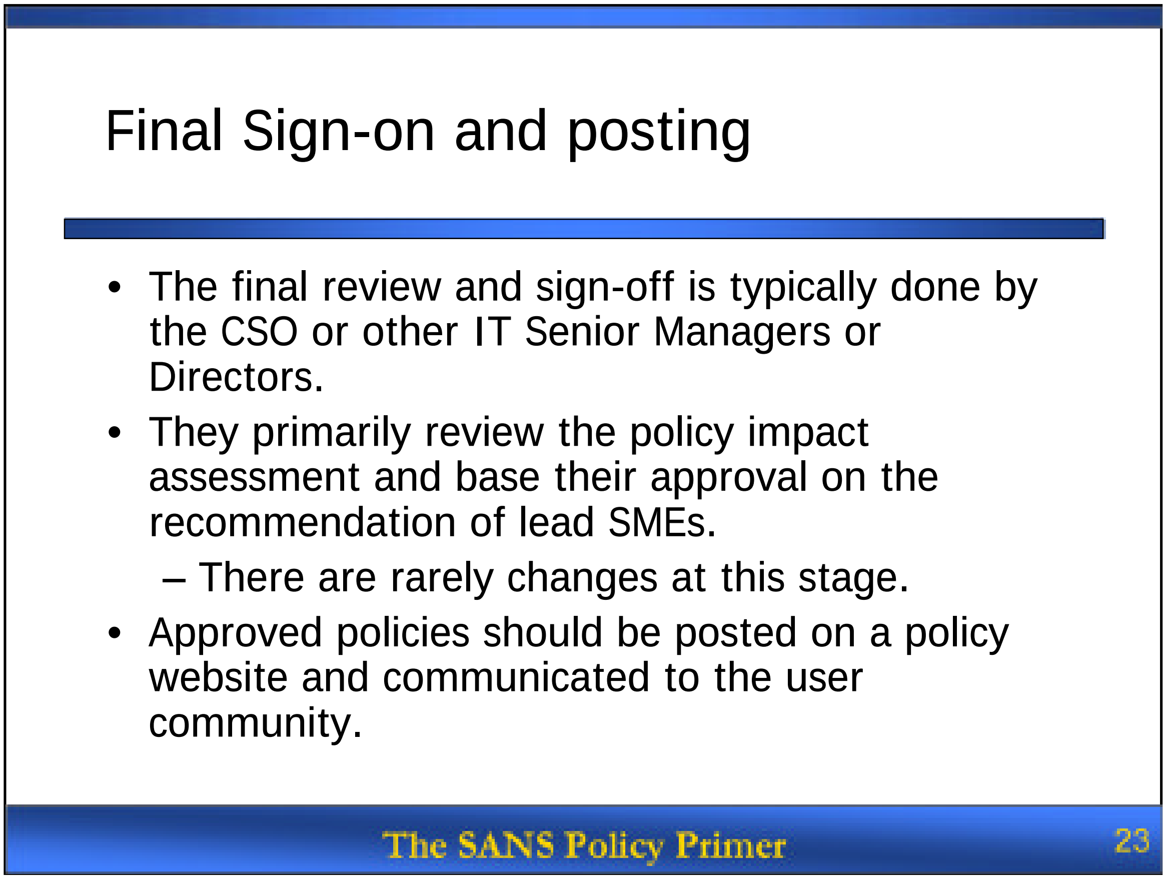
After the initial round of reviews, the policy would undergo a review by a wider audience with the security function. This would include managers as well as individual contributors. Once the review is completed at this stage, the policy is ready to be sent to HR and Legal for review.



HR and Legal Review

- The primary legal and HR representatives review the updated policy and/or standards.
- They are looking specifically at
  - Privacy issues
  - Legal policy issues
  - HR enforcement language
- Typically there not any changes to the policy at this point. Any necessary changes at this stage should be minimal and not change the intent of the policy.

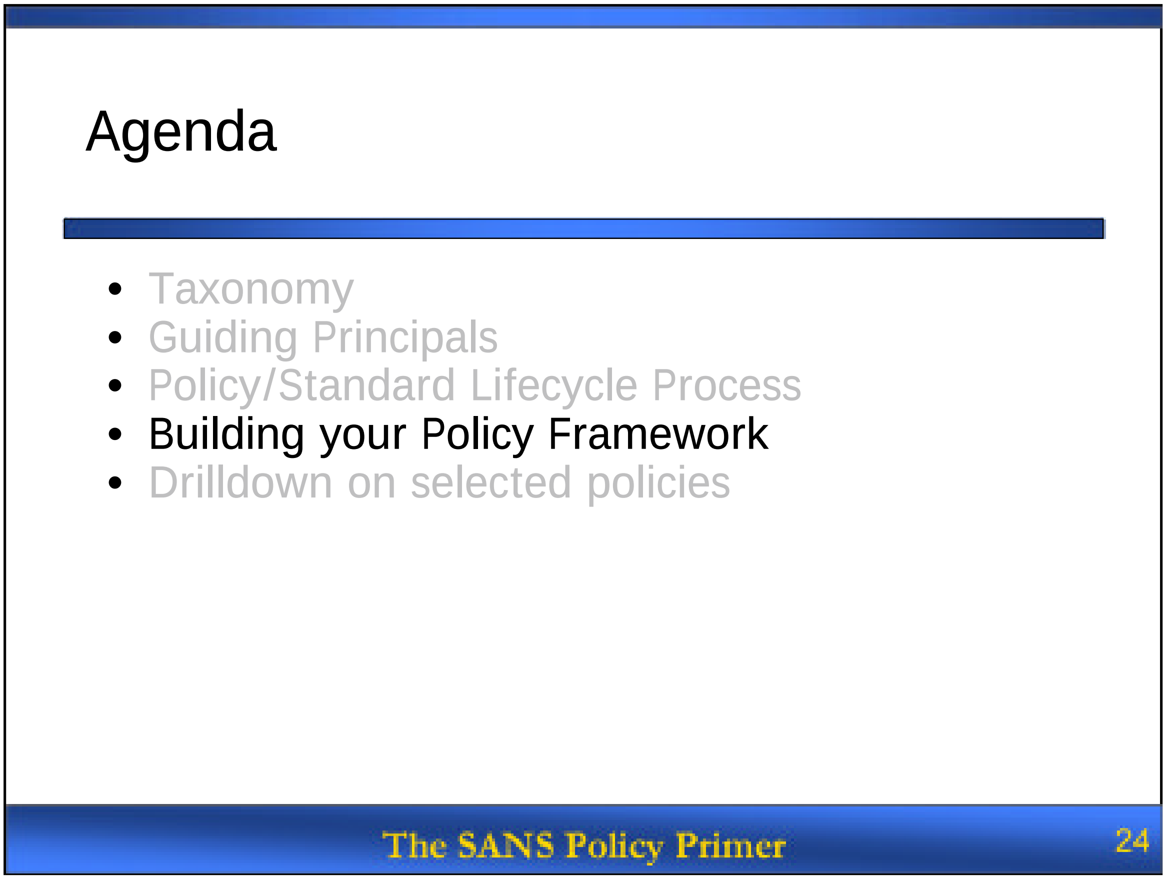
Legal and HR review of policies is required in many, if not most, organizations. Often, this may just be a formality, but it could play a crucial role in defending the company against civil lawsuits in the future. Ideally, you want to have the same person from legal and HR be assigned to review each policy. Once the policy review is completed at this stage, the policy is ready for the steering committee or final sign-off.



Final Sign-on and posting

- The final review and sign-off is typically done by the CSO or other IT Senior Managers or Directors.
- They primarily review the policy impact assessment and base their approval on the recommendation of lead SMEs.
  - There are rarely changes at this stage.
- Approved policies should be posted on a policy website and communicated to the user community.

The final review stage of a policy is almost a rubber-stamp sign-off. At this point, the policy should have been reviewed by enough technical leads that any red-flags would have been raised and addressed. The CSO or other senior managers who sign-off on the policy usually do so on the recommendation of the senior SMEs. Top-level management review and sign-off is necessary since they are the ones who are accountable for enforcing the policy.



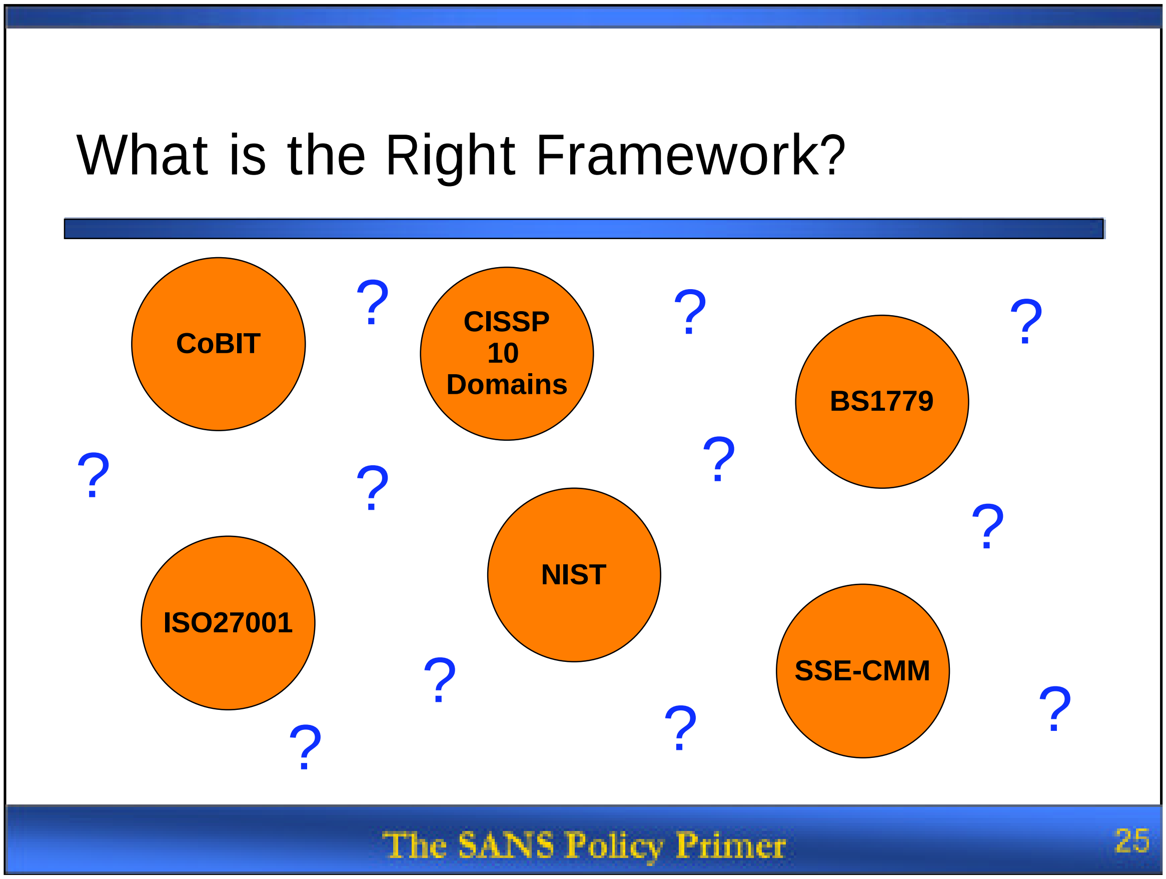
Agenda

- Taxonomy
- Guiding Principals
- Policy/Standard Lifecycle Process
- Building your Policy Framework
- Drilldown on selected policies

The SANS Policy Primer 24

In this section we are going to look at building a policy framework. We will cover the following topics:

- What is the Right Framework
- Key Policies Every Organization Needs
- Example Policy Template
- Policy Drilldowns



What is the Right Framework?

CoBIT

CISSP 10 Domains

BS1779

ISO27001

NIST

SSE-CMM

The SANS Policy Primer 25

There are a number of standards and certifications that can be used as the basis for your policy framework.

CoBIT - The Control Objectives for Information and related Technology. This is a set of best practices for IT Management.

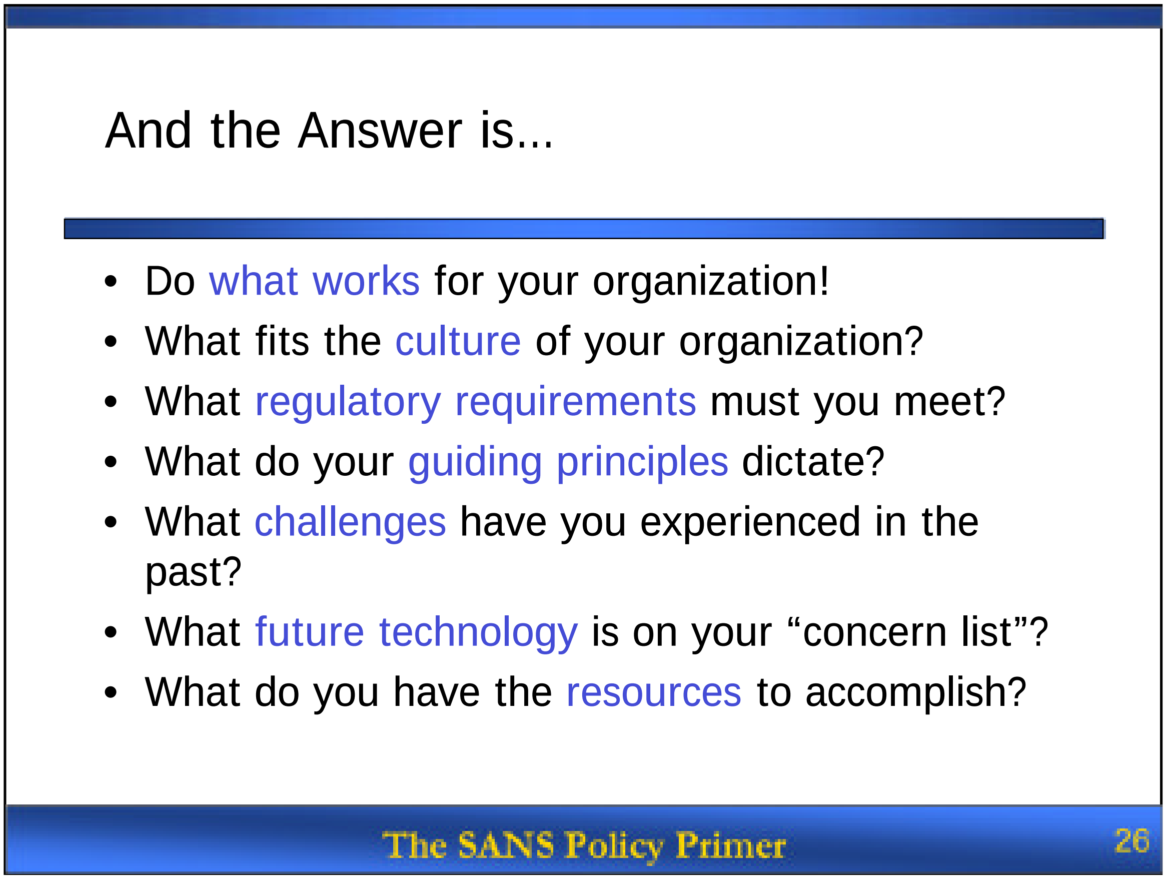
ISO27001 - Information Security Management - Specification With Guidance for Use, is the replacement for BS7799-2. It is intended to provide the foundation for third party audit, and is 'harmonized' with other management standards, such as ISO 9001 and ISO 14001. (From the ISO27001 website)

BS1799 - Business Continuity Planning ISO 17799 (Ten domains)

NIST – National Institute of Standards and Technology

SSE-CMM – Systems Security Engineer Capability Maturity Model

CISSP – Certified Information Systems Security Professional (10 domains)

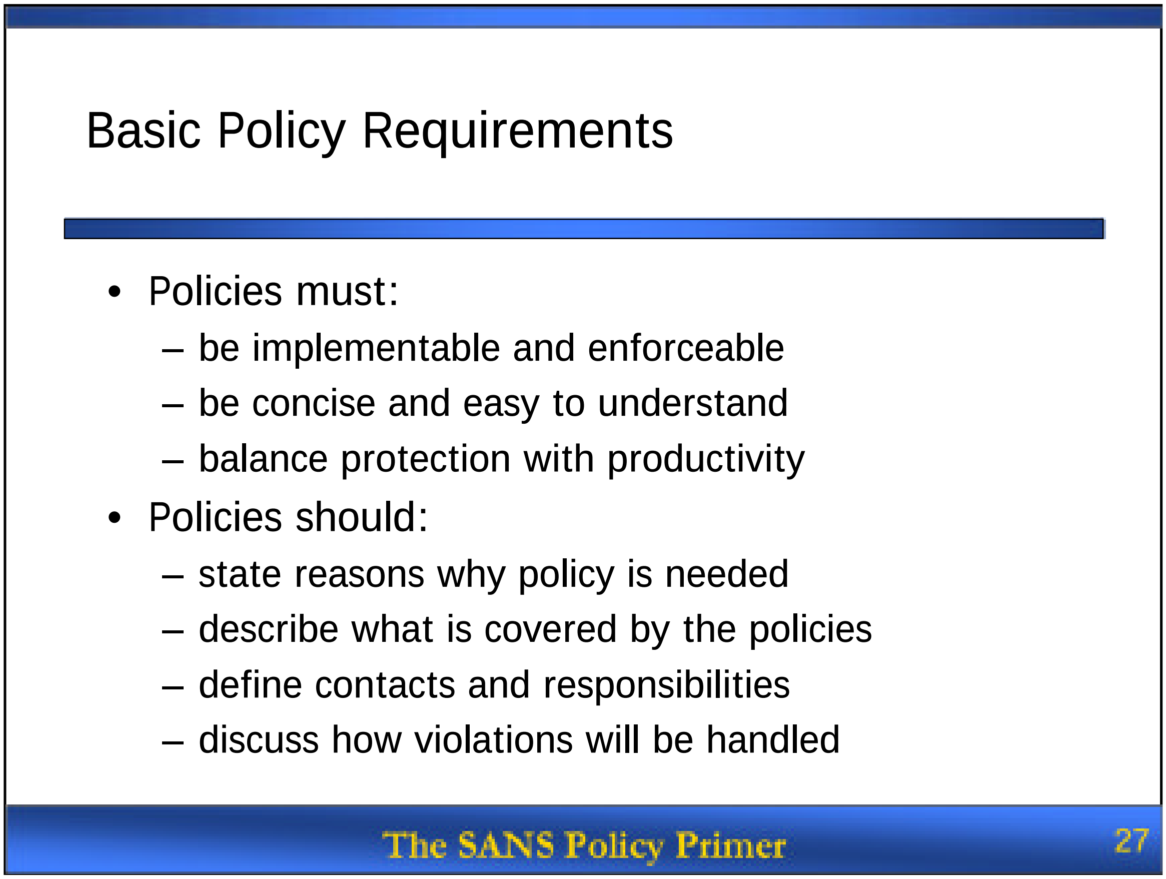


And the Answer is...

- Do what works for your organization!
- What fits the culture of your organization?
- What regulatory requirements must you meet?
- What do your guiding principles dictate?
- What challenges have you experienced in the past?
- What future technology is on your “concern list”?
- What do you have the resources to accomplish?

The SANS Policy Primer 26

Choosing the right policy framework is all about what will work best for your organization. You need to consider the culture of your organization, the established guiding principles, challenges you may have experienced in the past and what resources you will have for the policy management function. Also, very critical to consider what regulatory requirements you must meet.

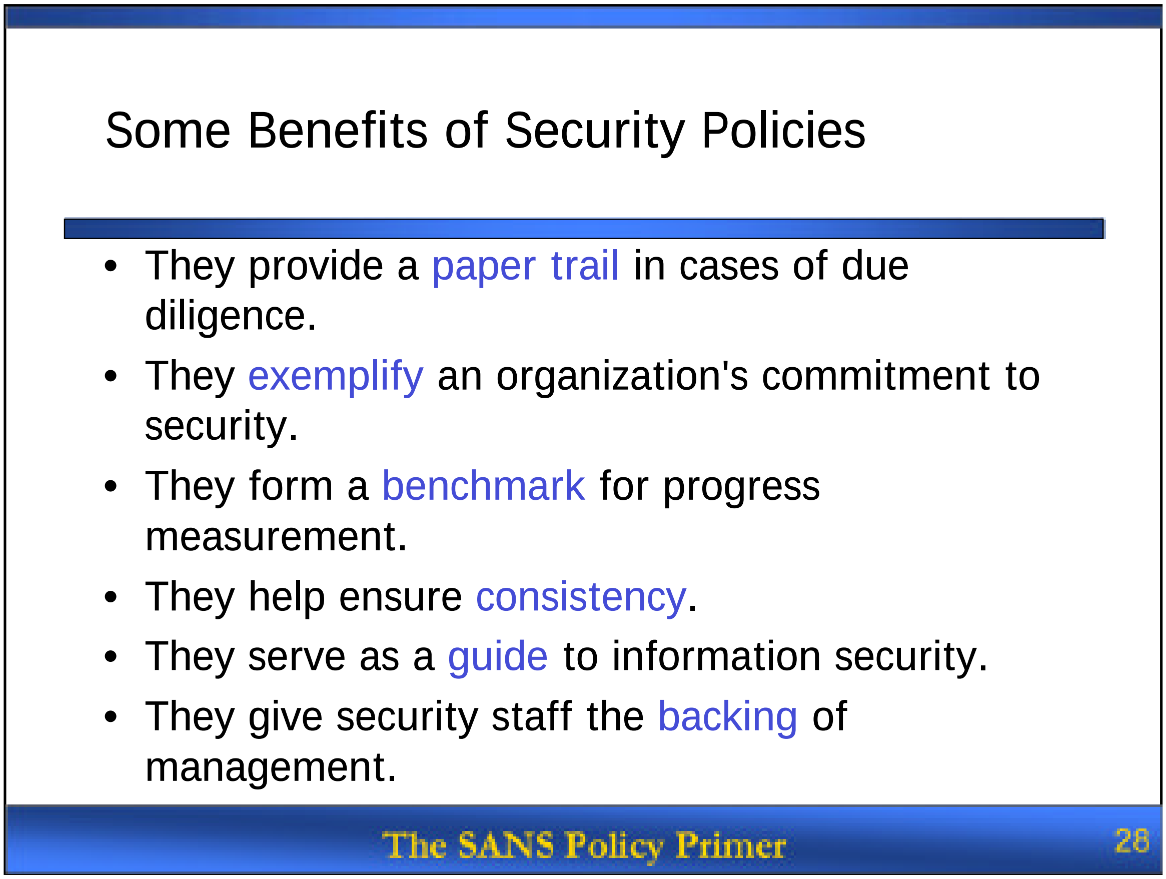


Basic Policy Requirements

- Policies must:
  - be implementable and enforceable
  - be concise and easy to understand
  - balance protection with productivity
- Policies should:
  - state reasons why policy is needed
  - describe what is covered by the policies
  - define contacts and responsibilities
  - discuss how violations will be handled

The SANS Policy Primer 27

This page discusses some basic rules for policies. While many of these may seem obvious, it is necessary to point them out. When planning policies, some organizations will go overboard with policies and come up with something that will be impossible to implement and comply with. The bottom line for policies is they must take into consideration the balance of protection with the impact to productivity . You also want policies to be concise and easy to read and understand. Our goal at Cisco is to keep policies to 2 pages or less, if at all possible. We do have a few policies which are 4 or 5 pages. One thing to keep in mind when developing a policy is how it will effect legacy systems and other infrastructure that is already in place. Once the policies are fully approved, they should be made available to all users who are affected. Finally, all policies should be updated annually to reflect changes in organization or culture.

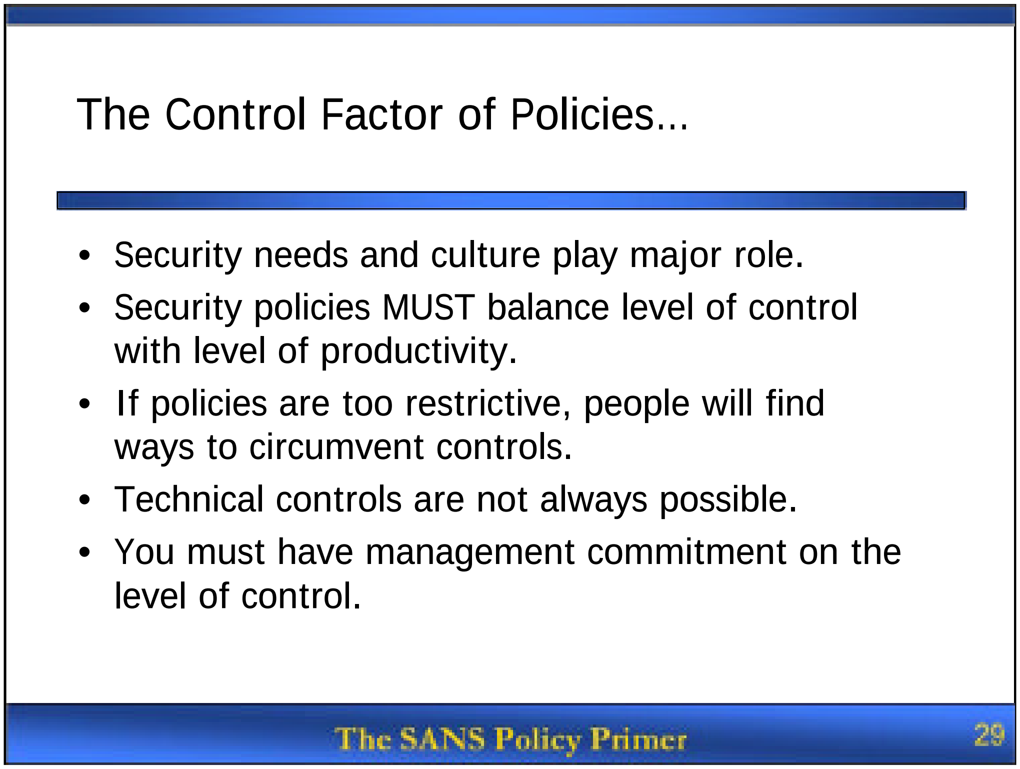


Some Benefits of Security Policies

- They provide a paper trail in cases of due diligence.
- They exemplify an organization's commitment to security.
- They form a benchmark for progress measurement.
- They help ensure consistency.
- They serve as a guide to information security.
- They give security staff the backing of management.

The SANS Policy Primer 28

Security policies are a must have for any organization, large or small. They provide the “glue” and foundation for the security framework. A few of the benefits of security policies are listed above. This is certainly not an exhaustive list.

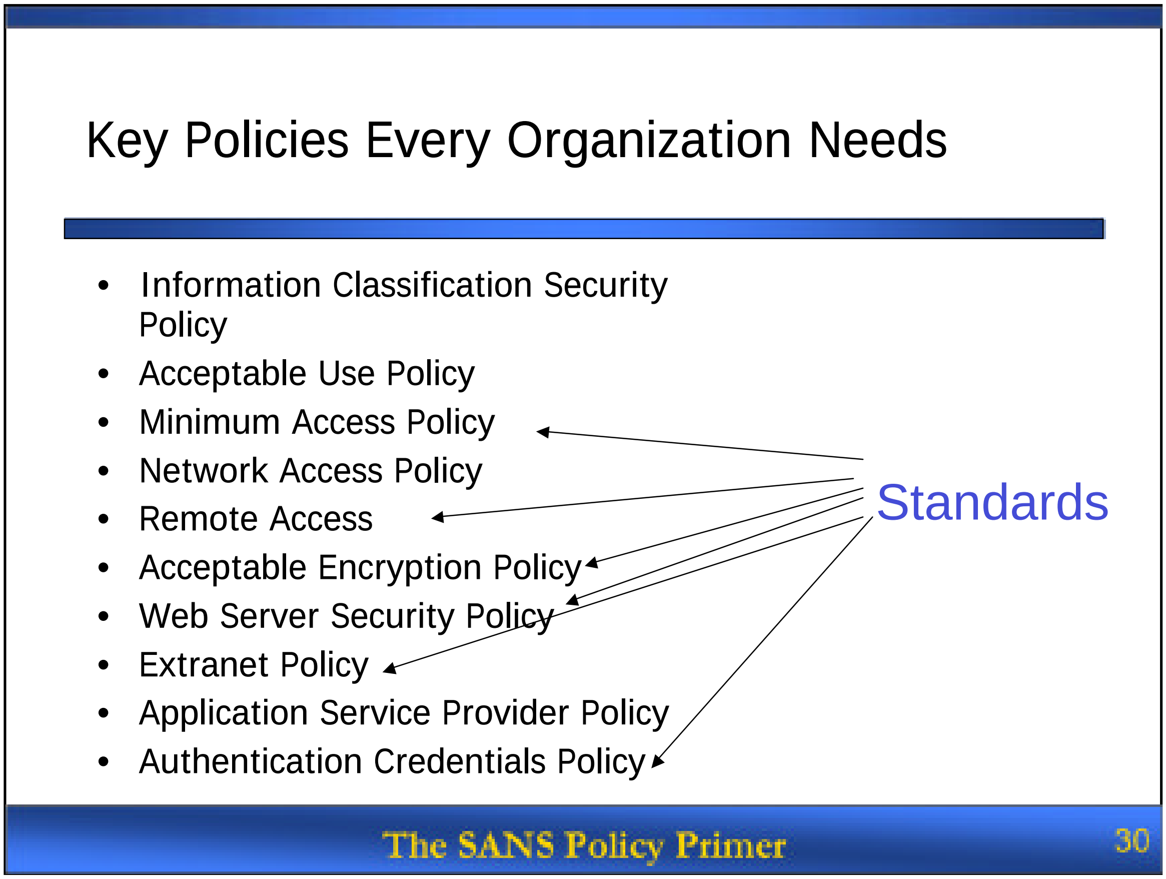


The Control Factor of Policies...

- Security needs and culture play major role.
- Security policies MUST balance level of control with level of productivity.
- If policies are too restrictive, people will find ways to circumvent controls.
- Technical controls are not always possible.
- You must have management commitment on the level of control.

The SANS Policy Primer 29

One of the major goal of a security policy is to implement control. Deciding on the level of control for a specific policy is not always clear-cut. The security needs and the culture of the organization will play a major role when deciding what level of control is appropriate. If you make policies too restrictive or too hard to implement and comply with, they will either be ignored (not implemented) or people will find a way to circumvent the controls in the policies.



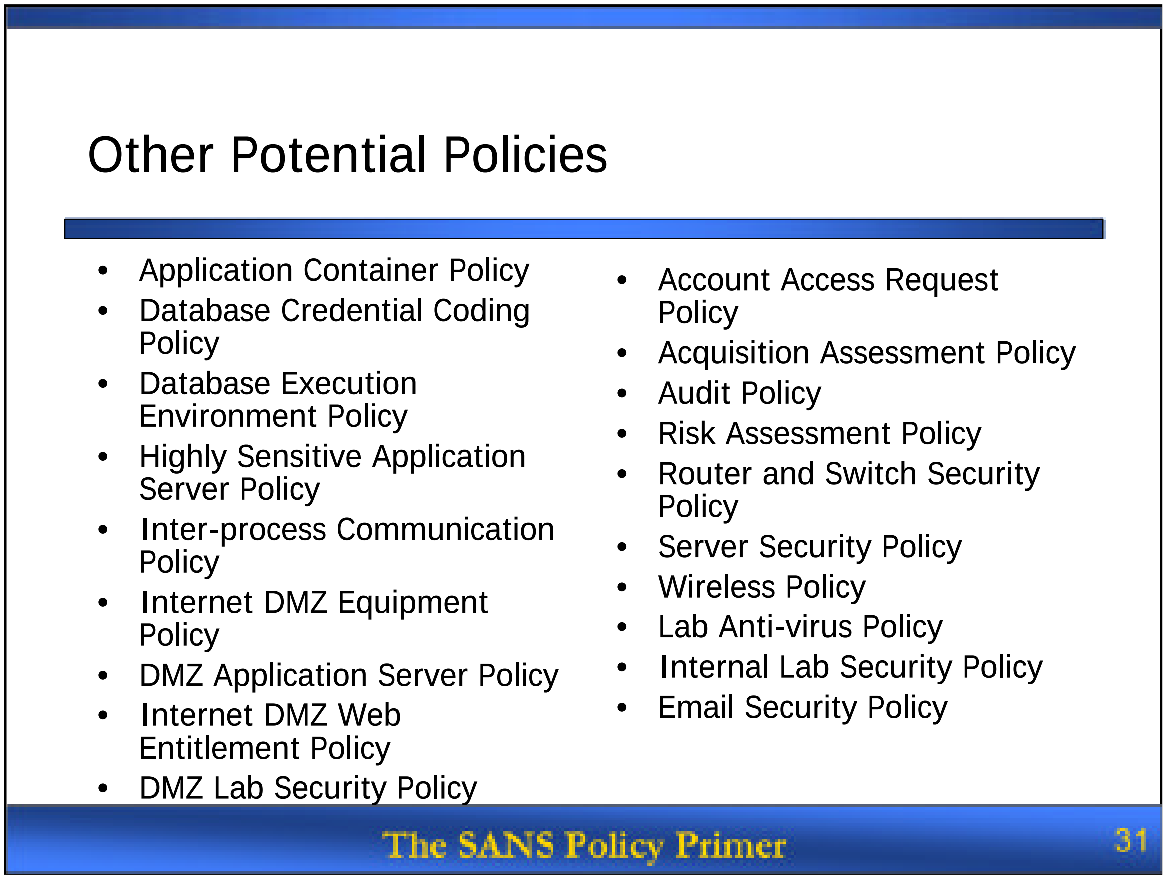
Key Policies Every Organization Needs

- Information Classification Security Policy
- Acceptable Use Policy
- Minimum Access Policy
- Network Access Policy
- Remote Access
- Acceptable Encryption Policy
- Web Server Security Policy
- Extranet Policy
- Application Service Provider Policy
- Authentication Credentials Policy

Standards

The SANS Policy Primer 30

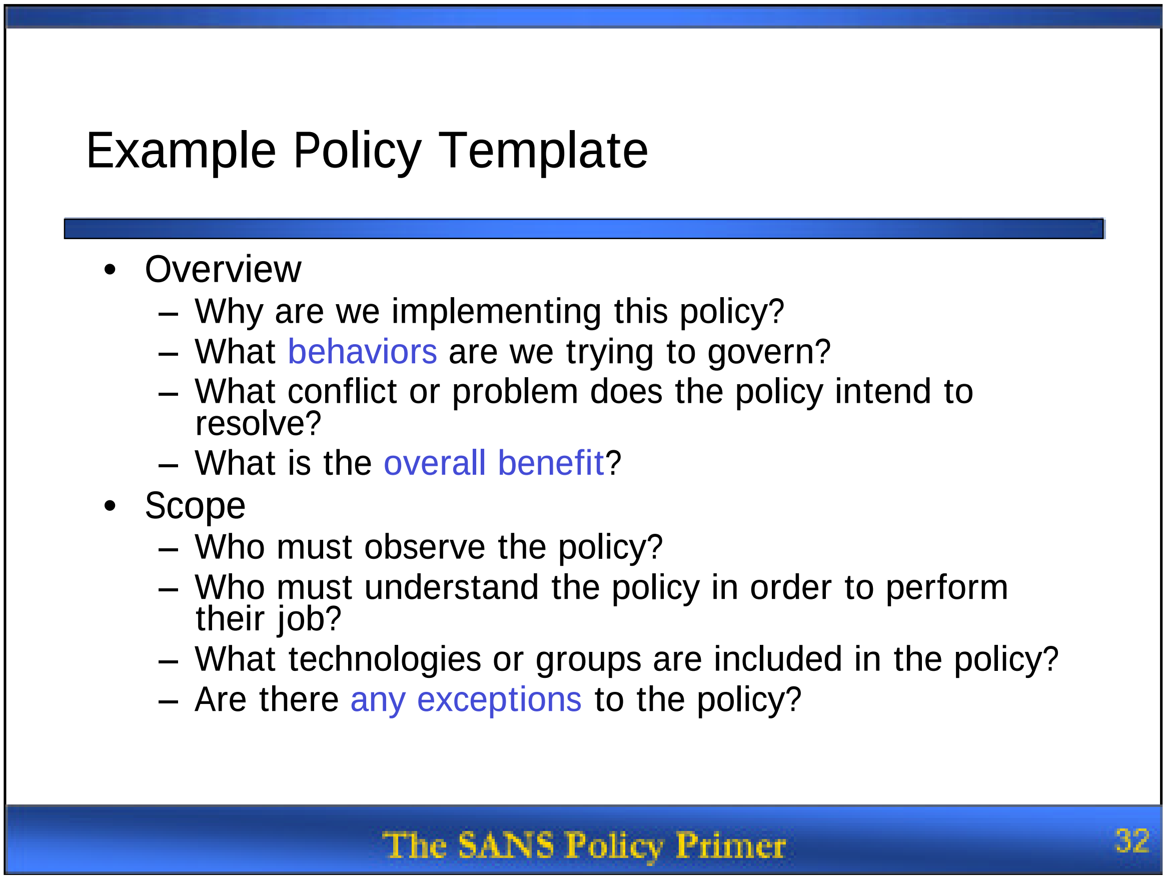
The policies listed here are foundational key policies that almost any organization that has internet presence will need. Many of these policies will also have an associated standard. We will drilldown on some of these policies in the next section. You find examples of many of these policies (and more) on the SANS Policy website at: http://www.sans.org/resources/policies/



Other Potential Policies

- Application Container Policy
- Database Credential Coding Policy
- Database Execution Environment Policy
- Highly Sensitive Application Server Policy
- Inter-process Communication Policy
- Internet DMZ Equipment Policy
- DMZ Application Server Policy
- Internet DMZ Web Entitlement Policy
- DMZ Lab Security Policy
- Account Access Request Policy
- Acquisition Assessment Policy
- Audit Policy
- Risk Assessment Policy
- Router and Switch Security Policy
- Server Security Policy
- Wireless Policy
- Lab Anti-virus Policy
- Internal Lab Security Policy
- Email Security Policy

These are just a few more examples of policies that may be needed by an organization. You find examples of many of these policies (and more) on the SANS Policy website at: http://www.sans.org/resources/policies/

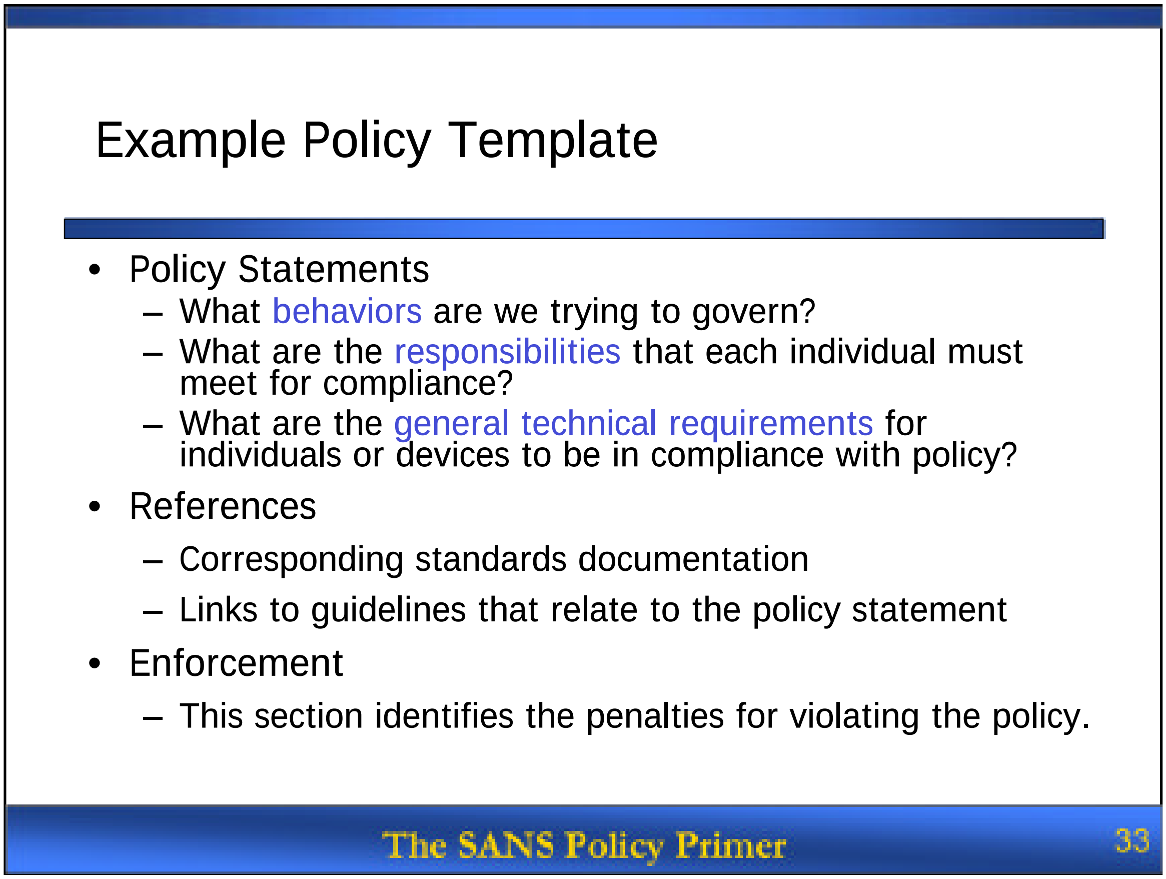


Example Policy Template

- Overview
  - Why are we implementing this policy?
  - What behaviors are we trying to govern?
  - What conflict or problem does the policy intend to resolve?
  - What is the overall benefit?
- Scope
  - Who must observe the policy?
  - Who must understand the policy in order to perform their job?
  - What technologies or groups are included in the policy?
  - Are there any exceptions to the policy?

The SANS Policy Primer 32

In these next few pages, we’ll look at some of the potential sections of a policy template. Developing a policy template should be one of the initial steps a security organization completes as part of developing their security policy framework. Having a policy template will ensure consistency throughout all of their policies.



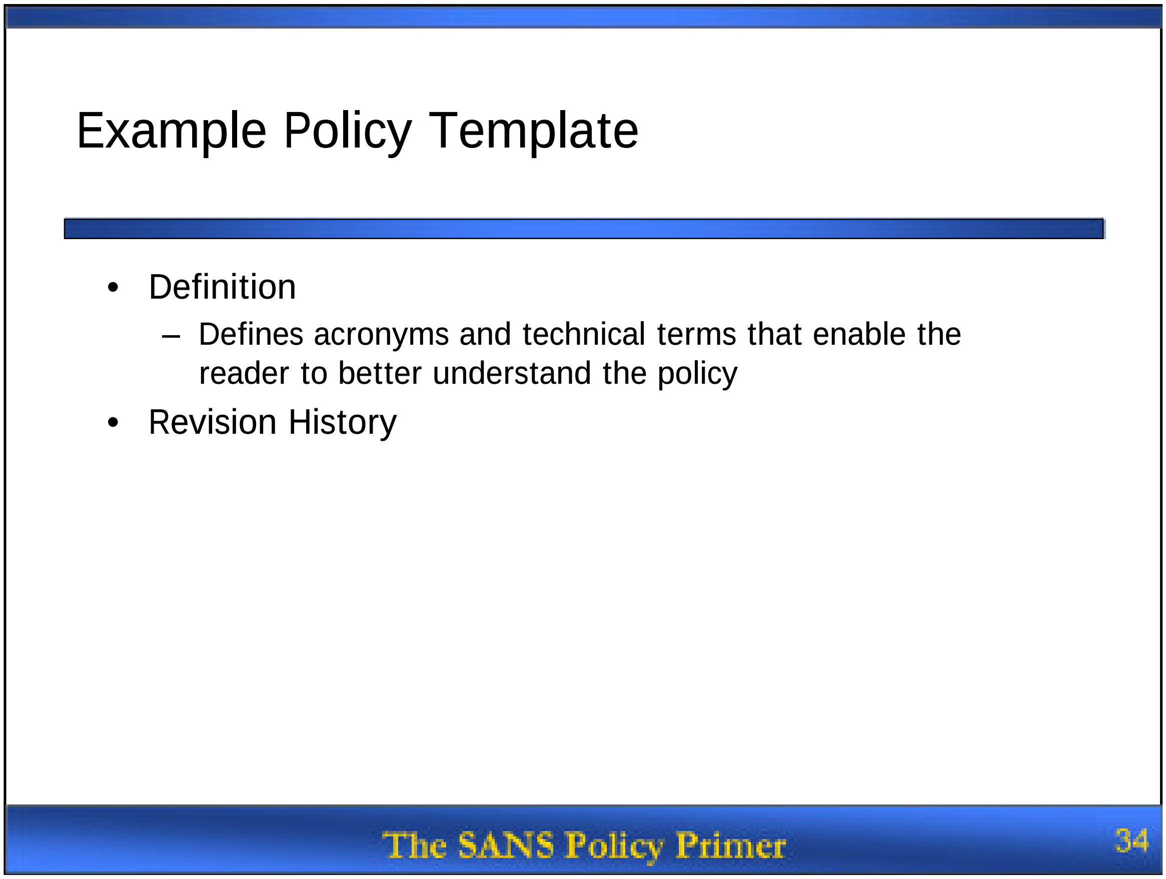
Example Policy Template

- Policy Statements
  - What behaviors are we trying to govern?
  - What are the responsibilities that each individual must meet for compliance?
  - What are the general technical requirements for individuals or devices to be in compliance with policy?
- References
  - Corresponding standards documentation
  - Links to guidelines that relate to the policy statement
- Enforcement
  - This section identifies the penalties for violating the policy.

The policy statement section of a policy is the most critical element. It is in this section where the must-have requirements and behaviors will be outlined.

The reference section should list any corresponding standards or related policies. Ideally, the URL should be embedded in the document so people can easily located these corresponding documents.

The enforcement section should be standard phrasing provided by your legal department.



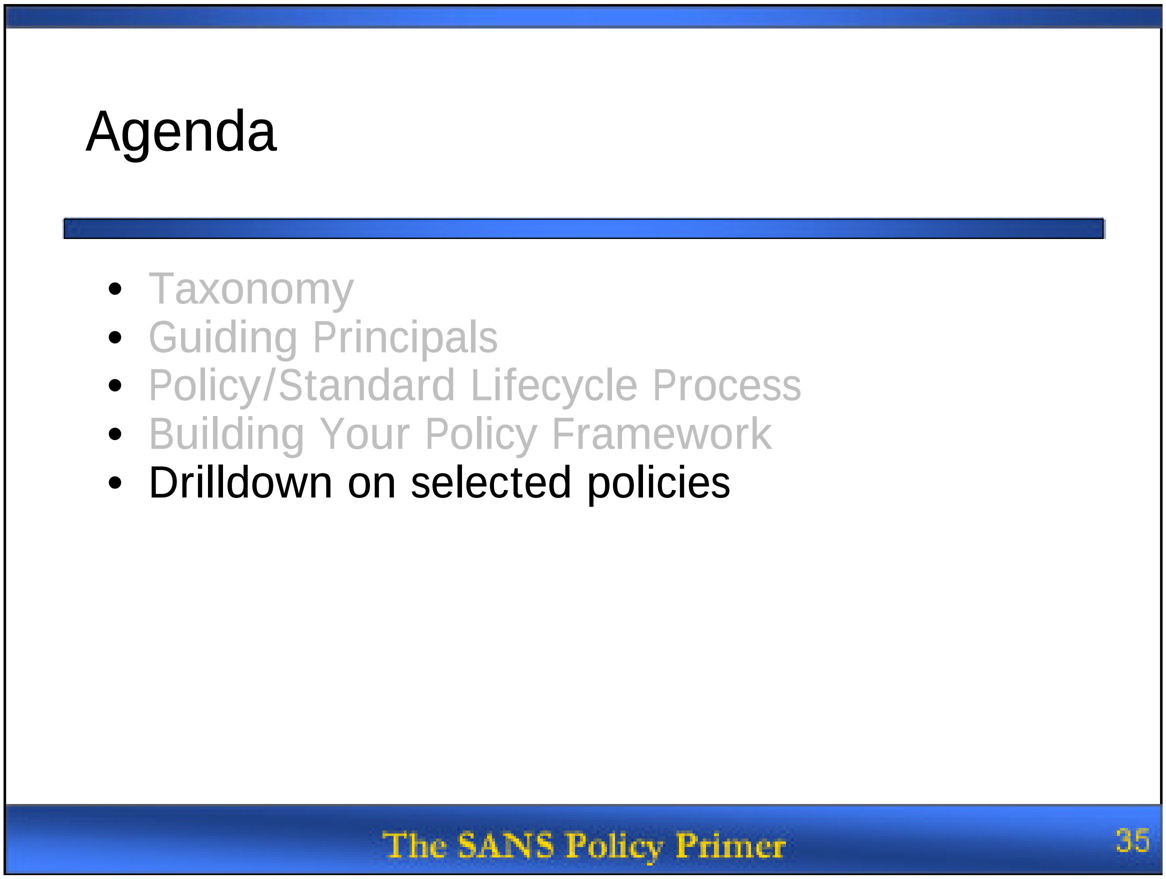
Example Policy Template

- Definition
  - Defines acronyms and technical terms that enable the reader to better understand the policy
- Revision History

The SANS Policy Primer 34

Unfamiliar definitions should be defined in the definition section.

The Revision History section should contain a short summary of all the revisions made to the policy, starting with the initial implementation date.

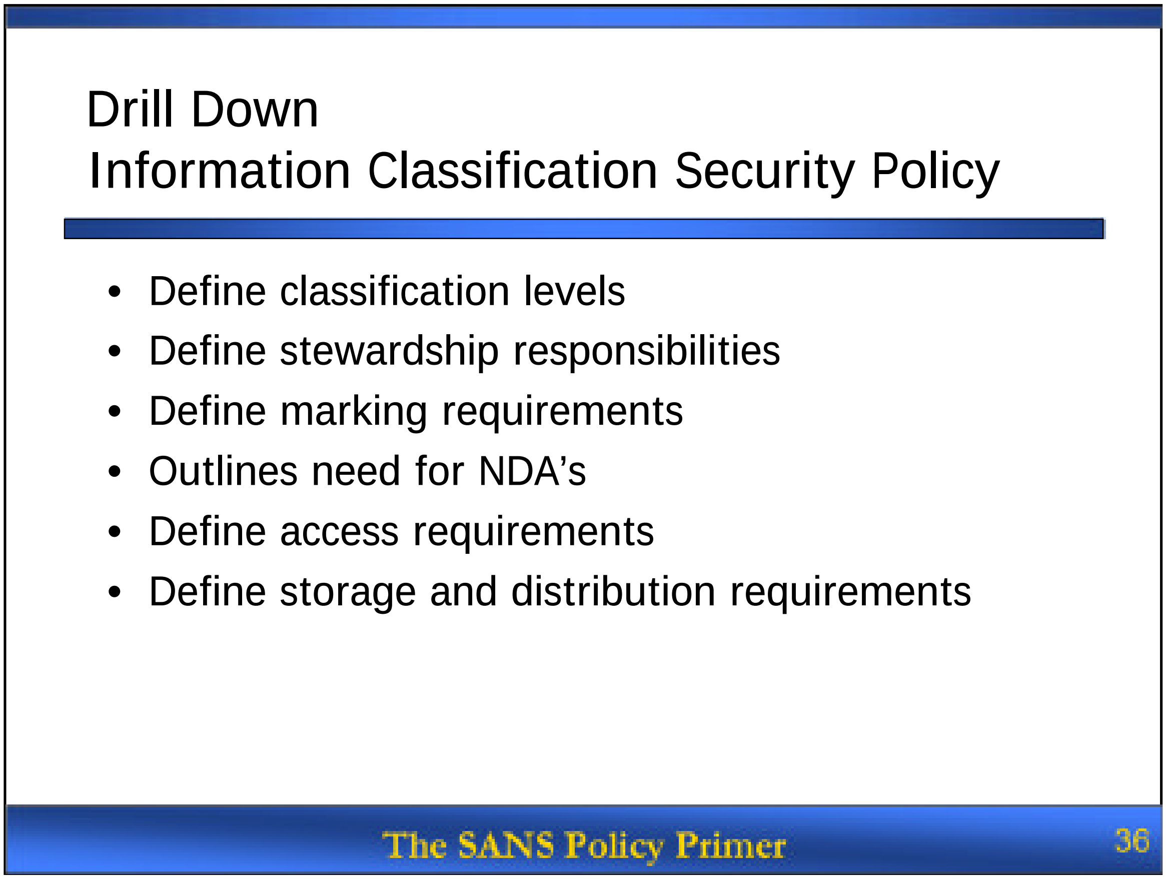


Agenda

- Taxonomy
- Guiding Principals
- Policy/Standard Lifecycle Process
- Building Your Policy Framework
- Drilldown on selected policies

The SANS Policy Primer 35

In this final section we will take a look at specific policies and some of the key elements required in each of these policies. These policies are available in Word or PDF format on the SANS policy website at: http://www.sans.org/resources/policies/

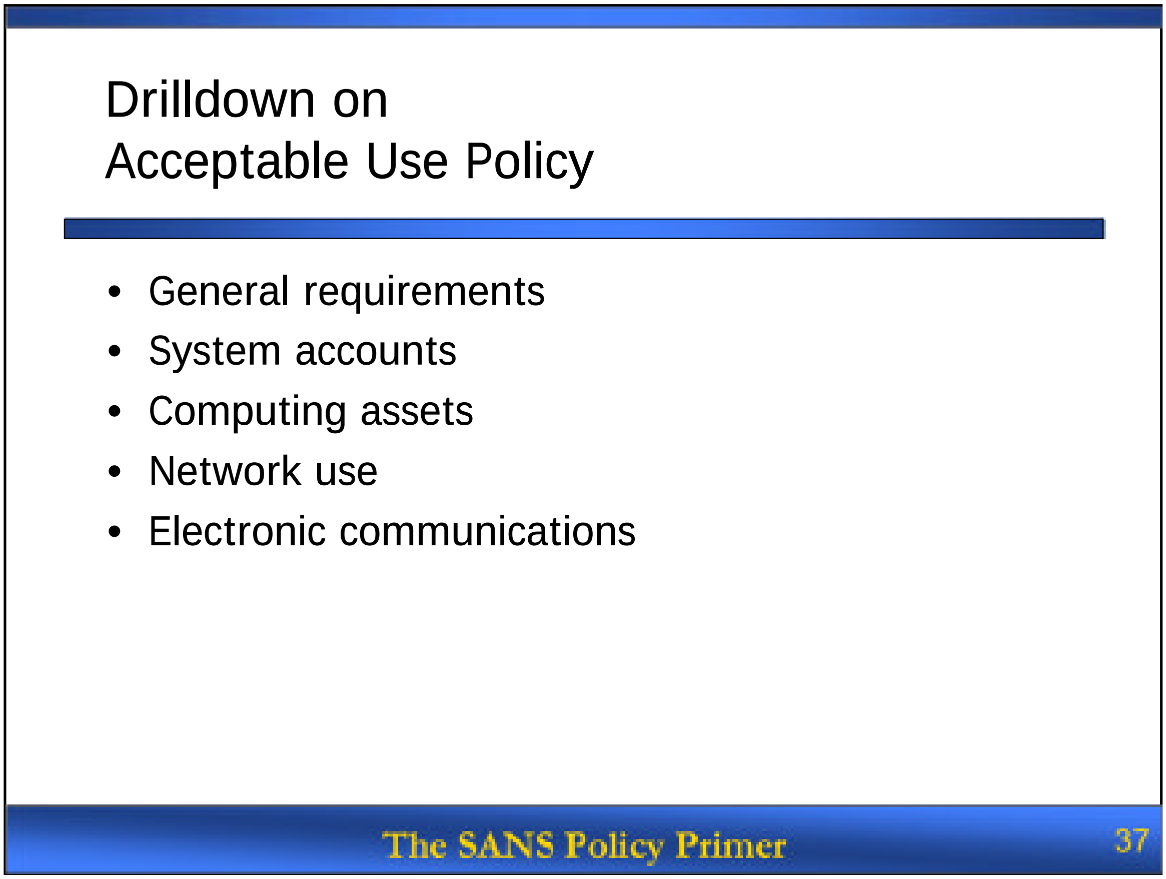


Drill Down
Information Classification Security Policy

- Define classification levels
- Define stewardship responsibilities
- Define marking requirements
- Outlines need for NDA’s
- Define access requirements
- Define storage and distribution requirements

The Information Classification Policy helps employees determine the relative sensitivity of information used by <Company Name>, and how this information should be treated and disclosed to other <Company Name>, employees and other parties

This policy applies to information stored or shared via any means and marked in accordance with this policy. This includes electronic information, information on paper, and information shared verbally or visually (such as telephone, whiteboards and video conferencing).



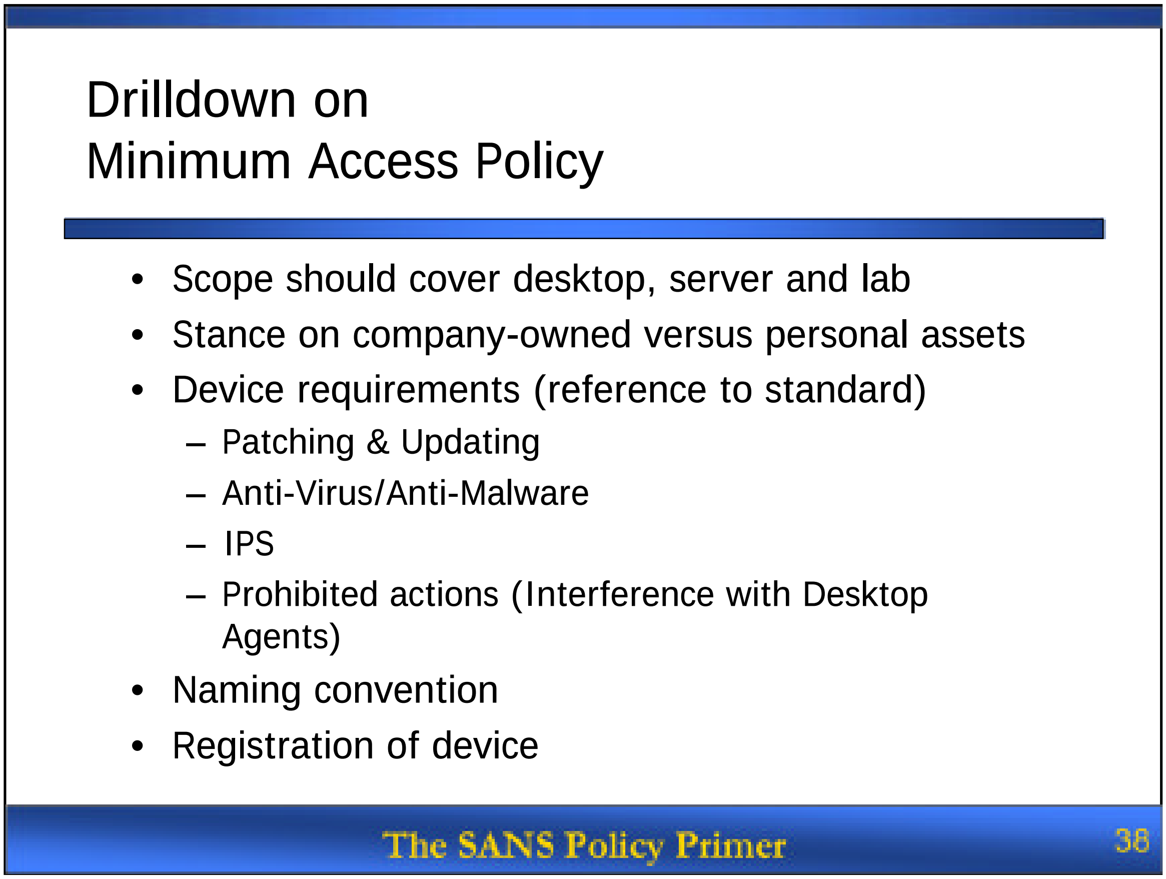
Drilldown on Acceptable Use Policy

- General requirements
- System accounts
- Computing assets
- Network use
- Electronic communications

The SANS Policy Primer 37

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 user and <Company Name>. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

Effective security is a team effort involving the participation and support of every user 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.



Drilldown on Minimum Access Policy

- Scope should cover desktop, server and lab
- Stance on company-owned versus personal assets
- Device requirements (reference to standard)
  - Patching & Updating
  - Anti-Virus/Anti-Malware
  - IPS
  - Prohibited actions (Interference with Desktop Agents)
- Naming convention
- Registration of device

The SANS Policy Primer 38

Some examples of prohibitive actions:

Using local workstation accounts to avoid domain login scripts or management.

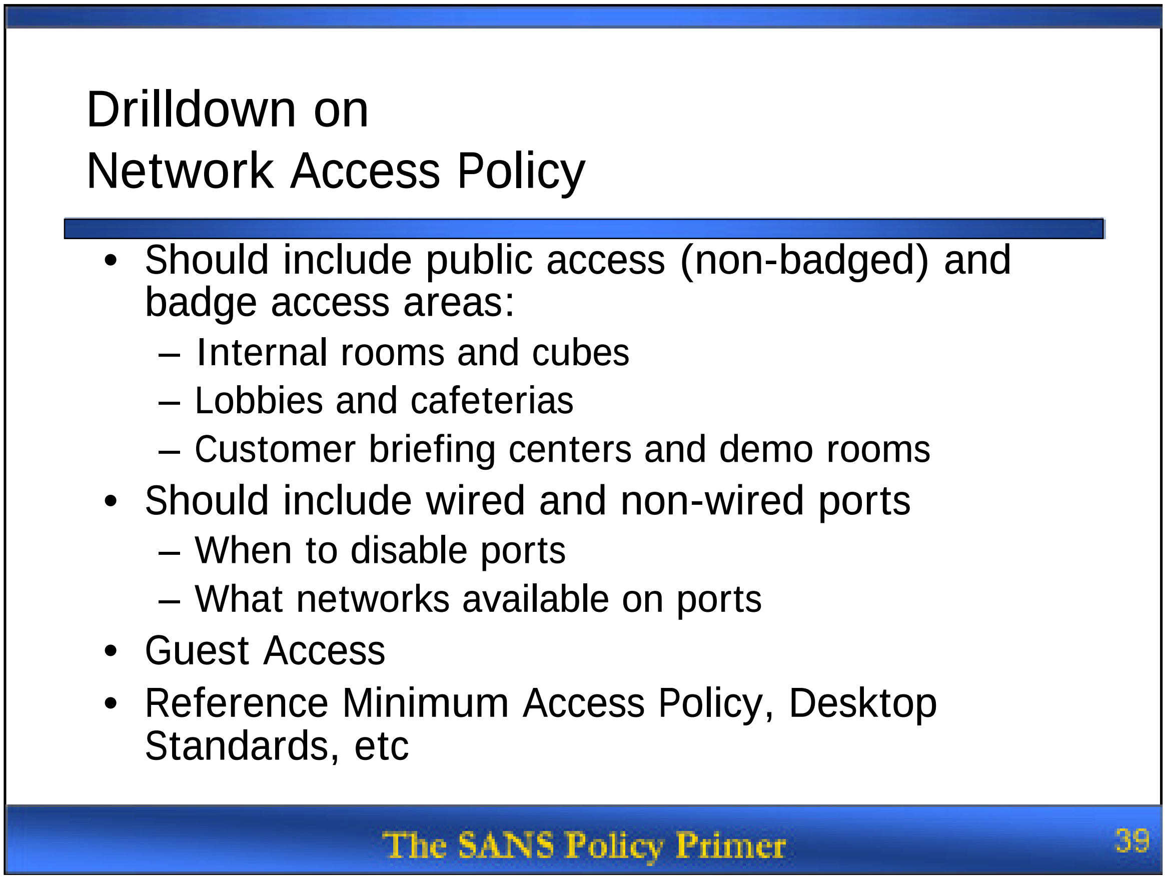
Modifying the default file associations of vbs, js, wsh, cmd and bat to block script execution.

Clearing the login script attribute from non-administrative/service accounts.

Reverse engineering for the purpose of restricting login script functionality.

Disabling services either comprising or supporting the desktop management agents.

Blocking agents’ required addresses, ports or protocols from inbound/outbound communication.

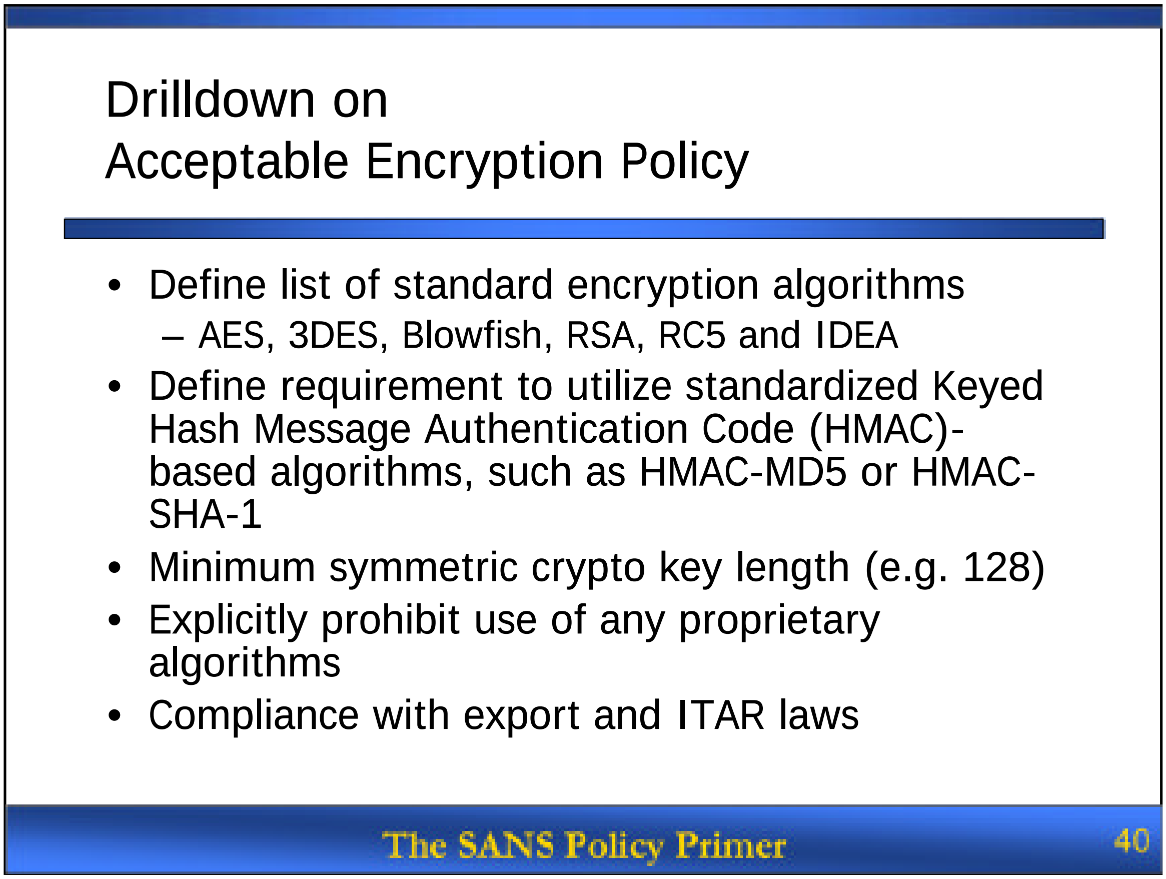


Drilldown on Network Access Policy

- Should include public access (non-badged) and badge access areas:
  - Internal rooms and cubes
  - Lobbies and cafeterias
  - Customer briefing centers and demo rooms
- Should include wired and non-wired ports
  - When to disable ports
  - What networks available on ports
- Guest Access
- Reference Minimum Access Policy, Desktop Standards, etc

This policy defines port access standards for all wired and wireless network data ports within any <Company Name> owned or operated facility. These standards will minimize the potential exposure to risk of the loss of (or damage to) sensitive or company confidential data, intellectual property, company image, etc., which might result from the unauthorized use of <Company Name> resources.

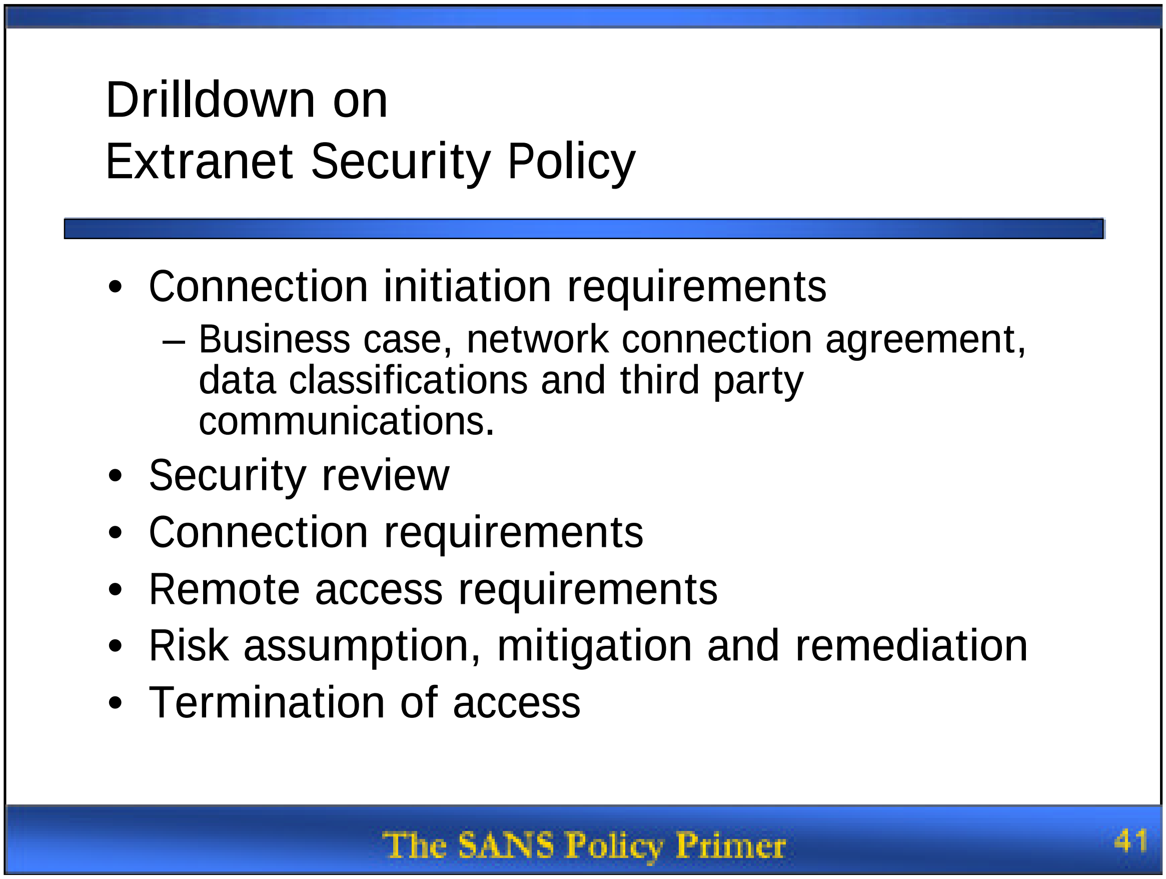
The purpose of this policy is to ensure the security of the entire <Company Name> network and the data that resides within it. This policy identifies the standards on the physical network in public and Access Card areas for wired and wireless network ports and their connections throughout all owned and operated <company Name> facilities connected to the <Company Name> network.



Drilldown on Acceptable Encryption Policy

- Define list of standard encryption algorithms
  - AES, 3DES, Blowfish, RSA, RC5 and IDEA
- Define requirement to utilize standardized Keyed Hash Message Authentication Code (HMAC)-based algorithms, such as HMAC-MD5 or HMAC-SHA-1
- Minimum symmetric crypto key length (e.g. 128)
- Explicitly prohibit use of any proprietary algorithms
- Compliance with export and ITAR laws

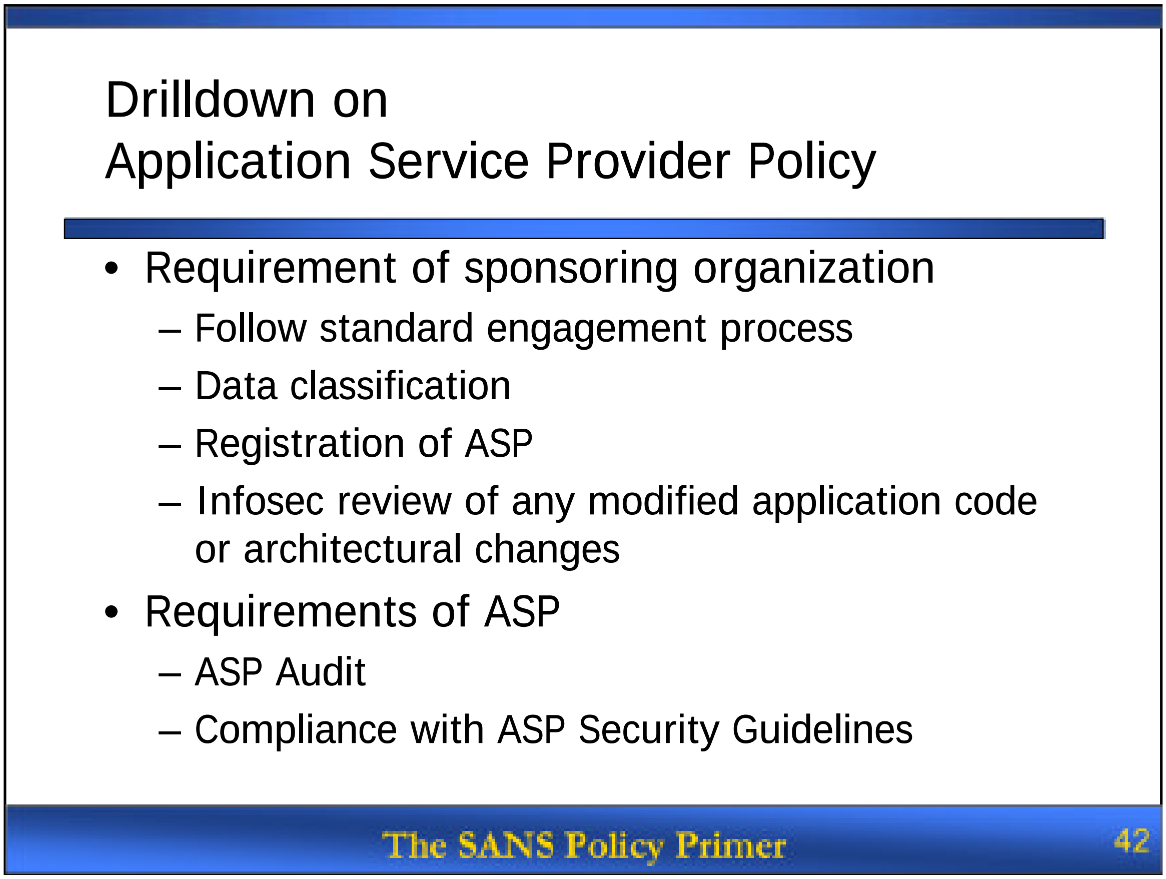
The purpose of this policy is to provide guidance which limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.



Drilldown on Extranet Security Policy

- Connection initiation requirements
  - Business case, network connection agreement, data classifications and third party communications.
- Security review
- Connection requirements
- Remote access requirements
- Risk assumption, mitigation and remediation
- Termination of access

This document sets forth the security requirements and processes pursuant to which Third Party organizations must adhere before they may connect to <Company Name> networks for the purpose of transacting business with or on behalf of <Company Name>.



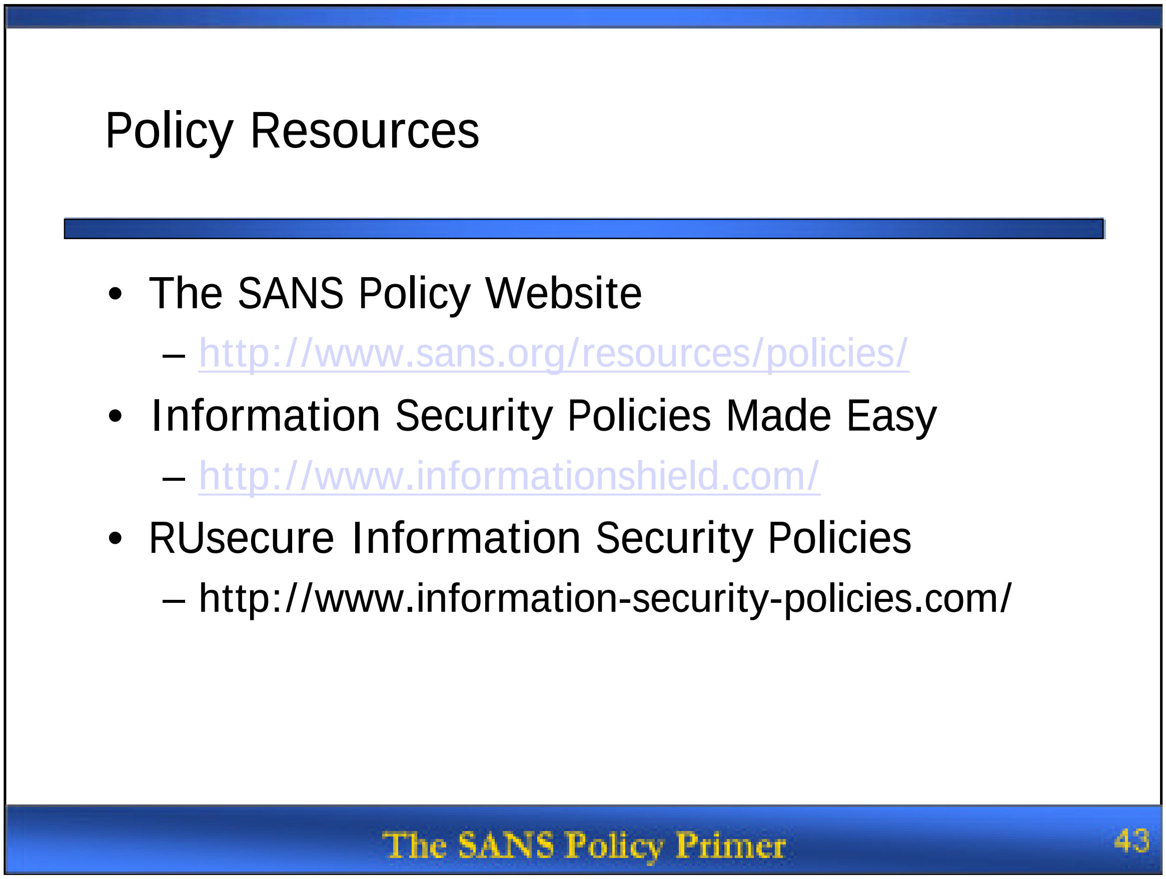
Drilldown on Application Service Provider Policy

- Requirement of sponsoring organization
  - Follow standard engagement process
  - Data classification
  - Registration of ASP
  - Infosec review of any modified application code or architectural changes
- Requirements of ASP
  - ASP Audit
  - Compliance with ASP Security Guidelines

The SANS Policy Primer 42

This policy applies to any use of Application Service Providers by <Company Name>, independent of where hosted.

It should outline the requirements of the sponsoring organization as well as the ASP.



Policy Resources

- The SANS Policy Website
  - – http://www.sans.org/resources/policies/
- Information Security Policies Made Easy
  - – http://www.informationshield.com/
- RUsecure Information Security Policies
  - – http://www.information-security-policies.com/

The SANS Policy Primer 43

This page left intentionally blank.