Management of Information Security

Chapter 4
Information Security Policy

Each problem that I solved became a rule which served afterwards to solve other problems

-- RENE DESCARTES (1596–1650)
“DISCOURS DE LA METHODE”

Learning Objectives

- ♦ Upon completion of this chapter, you should be able to:
  - – Define information security policy and understand its central role in a successful information security program
  - – Know the three major types of information security policy often used and what goes into each type
  - – Develop, implement, and maintain various types of information security policies

Introduction

- This chapter focuses on information security policy:
  - What it is
  - How to write it
  - How to implement it
  - How to maintain it

Introduction (Continued)

- Policy: essential foundation of effective information security program:

  “The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated systems.

  You, the policy maker, set the tone and the emphasis on how important a role information security will have within your agency.

  Your primary responsibility is to set the information resource security policy for the organization with the objectives of reduced risk, compliance with laws and regulations and assurance of operational continuity, information integrity, and confidentiality.”

Why Policy?

- A quality information security program begins and ends with policy
- Policies are least expensive means of control and often the most difficult to implement
- Some basic rules must be followed when shaping a policy:
  - Never conflict with law
  - Stand up in court
  - Properly supported and administered
  - Contribute to the success of the organization
  - Involve end users of information systems

Figure 4-1
The Bulls-eye Model

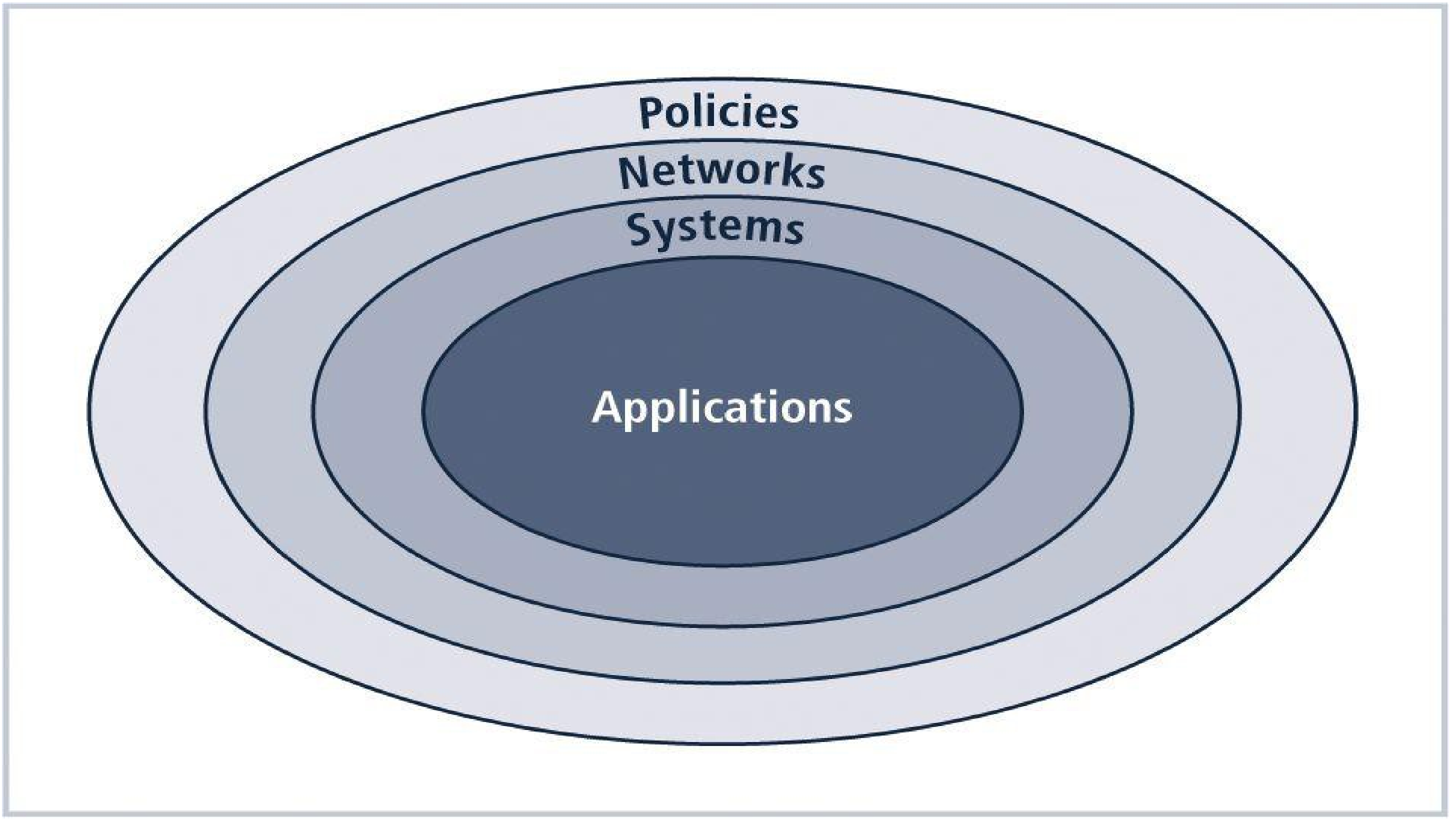


FIGURE 4-1 The Bull's-Eye Model

Policy Centric Decision Making

- Bulls-eye model layers:
  - Policies: first layer of defense
  - Networks: threats first meet organization’s network
  - Systems: computers and manufacturing systems
  - Applications: all applications systems
- Policies are important reference documents for internal audits and for resolution of legal disputes about management's due diligence
  - Policy documents can act as a clear statement of management's intent

Figure 4-2
Policies, Standards, & Practices

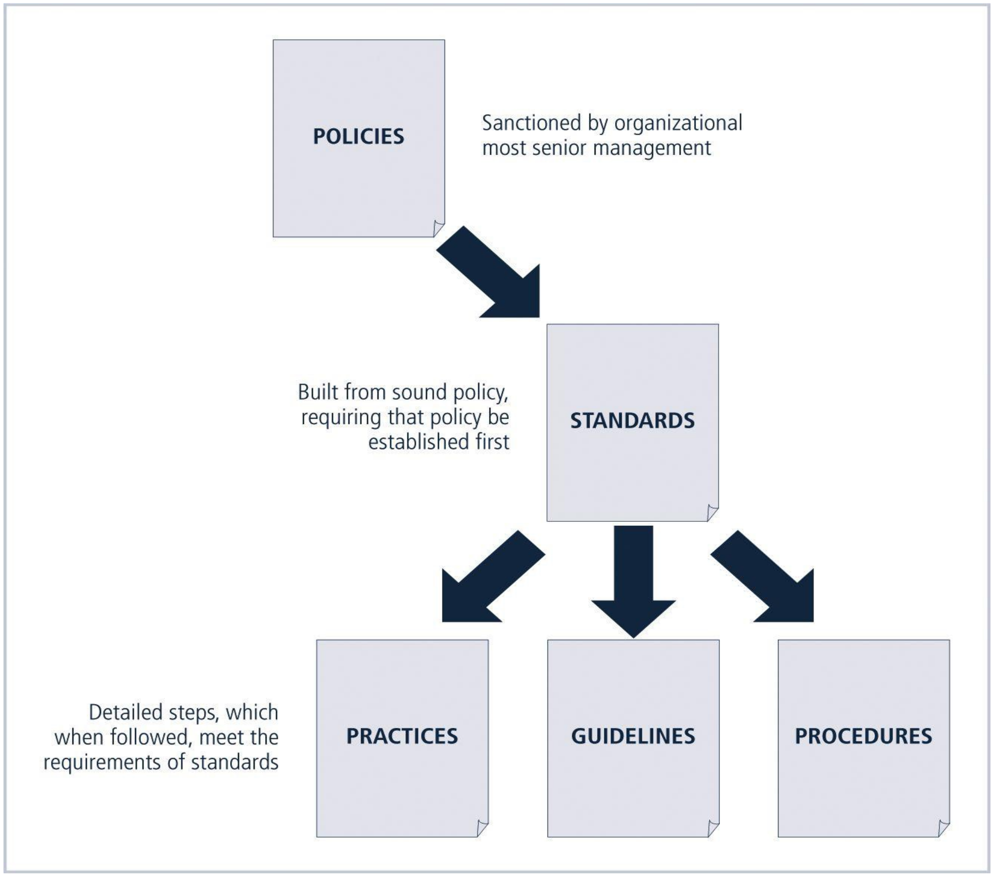

POLICIES
Sanctioned by organizational most senior management
Built from sound policy, requiring that policy be established first
STANDARDS
Detailed steps, which when followed, meet the requirements of standards
PRACTICES
GUIDELINES
PROCEDURES

FIGURE 4-2 Policies, Standards, and Practices

Policy, Standards, and Practices

- Policy: plan or course of action that influences and determines decisions
- Standards: more detailed statement of what must be done to comply with policy
- Practices, procedures and guidelines: explain how employees will comply with policy
- For policies to be effective, they must be:
  - Properly disseminated
  - Read
  - Understood
  - Agreed-to

Policy, Standards, and Practices (Continued)

- Policies require constant modification and maintenance

- In order to produce a complete information security policy, management must define three types of information security policy:
  - Enterprise information security program policy
  - Issue-specific information security policies
  - Systems-specific information security policies

Enterprise Information Security Policy (EISP)

- Sets strategic direction, scope, and tone for organization’s security efforts

- Assigns responsibilities for various areas of information security

- Guides development, implementation, and management requirements of information security program

EISP Elements

- EISP documents should provide :
  - An overview of corporate philosophy on security
  - Information about information security organization and information security roles
    - Responsibilities for security shared by all members of the organization
    - Responsibilities for security unique to each role within the organization

Components of the EISP

- Statement of Purpose: What the policy is for
- Information Technology Security Elements: Defines information security
- Need for Information Technology Security: justifies importance of information security in the organization
- Information Technology Security Responsibilities and Roles: Defines organizational structure
- References Information Technology standards and guidelines

Example EISP - CCW

- Protection Of Information: Information must be protected in a manner commensurate with its sensitivity, value, and criticality
- Use Of Information: Company X information must be used only for business purposes expressly authorized by management
- Information Handling, Access, And Usage: Information is a vital asset and all accesses to, uses of, and processing of Company X information must be consistent with policies and standards

Example EISP – CCW (Continued)

- Data And Program Damage Disclaimers: Company X disclaims any responsibility for loss or damage to data or software that results from its efforts to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems
- Legal Conflicts: Company X information security policies were drafted to meet or exceed the protections found in existing laws and regulations, and any Company X information security policy believed to be in conflict with existing laws or regulations must be promptly reported to Information Security management

Example EISP – CCW (Continued)

- Exceptions To Policies: Exceptions to information security policies exist in rare instances where a risk assessment examining the implications of being out of compliance has been performed, where a standard risk acceptance form has been prepared by the data Owner or management, and where this form has been approved by both Information Security management and Internal Audit management
- Policy Non-Enforcement: Management's non-enforcement of any policy requirement does not constitute its consent

Example EISP – CCW (Continued)

- Violation Of Law: Company X management must seriously consider prosecution for all known violations of the law
- Revocation Of Access Privileges: Company X reserves the right to revoke a user's information technology privileges at any time
- Industry-Specific Information Security Standards: Company X information systems must employ industry-specific information security standards

Example EISP – CCW (Continued)

- Use Of Information Security Policies And Procedures: All Company X information security documentation including, but not limited to, policies, standards, and procedures, must be classified as “Internal Use Only,” unless expressly created for external business processes or partners
- Security Controls Enforceability: All information systems security controls must be enforceable prior to being adopted as a part of standard operating procedure

Issue-Specific Security Policy (ISSP)

- Provides detailed, targeted guidance to instruct organization in secure use of technology systems
- Begins with introduction to fundamental technological philosophy of organization
- Serves to protect employee and organization from inefficiency/ambiguity
- Documents how technology-based system is controlled
  - Identifies processes and authorities that provide this control
- Serves to indemnify organization against liability for inappropriate or illegal system use

Issue-Specific Security Policy (ISSP)

- Every organization’s ISSP should:
  - Address specific technology-based systems
  - Require frequent updates
  - Contain an issue statement on the organization’s position on an issue
- ISSP topics could include:
  - E-mail, use of Internet and World Wide Web, specific minimum configurations of computers to defend against worms and viruses, prohibitions against hacking or testing organization security controls, home use of company-owned computer equipment, use of personal equipment on company networks, use of telecommunications technologies, use of photocopy equipment

Components of the ISSP

- Statement of Purpose
  - Scope and Applicability
  - Definition of Technology Addressed
  - Responsibilities
- Authorized Access and Usage of Equipment
  - User Access
  - Fair and Responsible Use
  - Protection of Privacy
- Prohibited Usage of Equipment
  - Disruptive Use or Misuse
  - Criminal Use
  - Offensive or Harassing Materials
  - Copyrighted, Licensed or other Intellectual Property
  - Other Restrictions

Components of the ISSP (Continued)

- Systems Management
  - Management of Stored Materials
  - Employer Monitoring
  - Virus Protection
  - Physical Security
  - Encryption
- Violations of Policy
  - Procedures for Reporting Violations
  - Penalties for Violations
- Policy Review and Modification
  - Scheduled Review of Policy and Procedures for Modification
- Limitations of Liability
  - Statements of Liability or Disclaimers

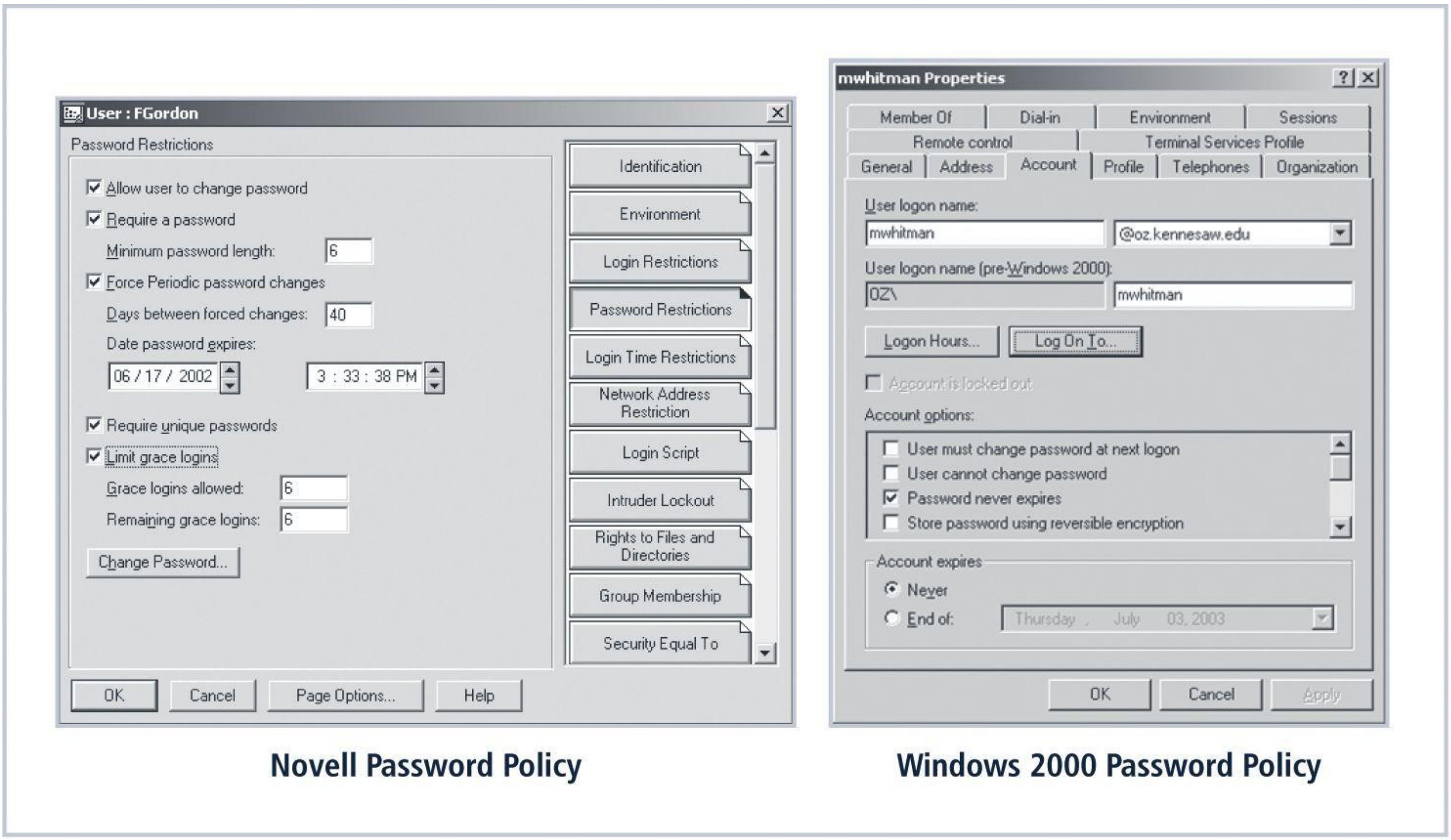
Implementing ISSP

- Common approaches:
  - Number of independent ISSP documents
  - Single comprehensive ISSP document
  - Modular ISSP document that unifies policy creation and administration
- Recommended approach is modular policy, which provides a balance between issue orientation and policy management

Systems-Specific Policy (SysSP)

- Systems-Specific Policies (SysSPs) frequently do not look like other types of policy
- They may often be created to function as standards or procedures to be used when configuring or maintaining systems
- SysSPs can be separated into:
  - Management guidance
  - Technical specifications
  - Combined in a single policy document

Figure 4-3
Password SysSP



User : FGordon

Password Restrictions

☑ Allow user to change password

☑ Require a password

Minimum password length: 6

☑ Force Periodic password changes

Days between forced changes: 40

Date password expires: 06 / 17 / 2002 3 : 33 : 38 PM

☑ Require unique passwords

☑ Limit grace logins

Grace logins allowed: 6

Remaining grace logins: 6

Novell Password Policy

mwhitman Properties

User logon name: mwhitman @oz.kennesaw.edu

User logon name (pre-Windows 2000): OZ\ mwhitman

□ Account is locked out

Account options:

□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Store password using reversible encryption

Account expires

● Never

○ End of: Thursday , July 03, 2003

Windows 2000 Password Policy

FIGURE 4-3 Password SysSP

Management Guidance SysSPs

- Created by management to guide the implementation and configuration of technology

- Applies to any technology that affects the confidentiality, integrity or availability of information

- Informs technologists of management intent

Technical Specifications SysSPs

- System administrators directions on implementing managerial policy
- Each type of equipment has its own type of policies
- Two general methods of implementing such technical controls:
  - Access control lists
  - Configuration rules

Access Control Lists

- Include user access lists, matrices, and capability tables that govern rights and privileges
- Can control access to file storage systems, object brokers or other network communications devices
- Capability Table: similar method that specifies which subjects and objects users or groups can access
- Specifications are frequently complex matrices, rather than simple lists or tables
- Level of detail and specificity (often called granularity) may vary from system to system
  - ACLs enable administrations to restrict access according to user, computer, time, duration, or even a particular file

ACLs

- In general ACLs regulate:
  - Who can use the system
  - What authorized users can access
  - When authorized users can access the system
  - Where authorized users can access the system from
  - How authorized users can access the system
  - Restricting what users can access, e.g. printers, files, communications, and applications

ACLs (Continued)

- Administrators set user privileges, such as:
  - Read
  - Write
  - Create
  - Modify
  - Delete
  - Compare
  - Copy

Configuration Rules

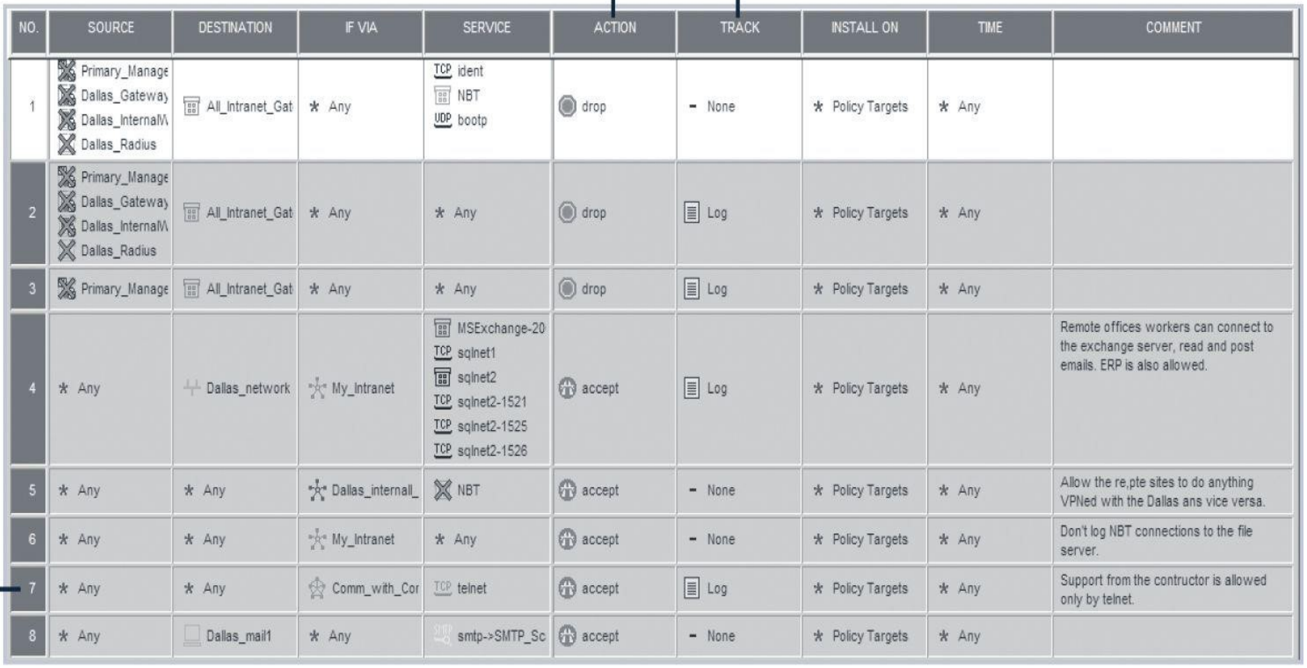
- Configuration rules are specific configuration codes entered into security systems to guide execution of system when information is passing through it
- Rule policies are more specific to system operation than ACLs and may or may not deal with users directly
- Many security systems require specific configuration scripts telling systems what actions to perform on each set of information processed

Figure 4-6
Firewall Configuration Rules

Action specifies whether the packet from Source: is accepted (allowed through) or dropped.

Track specifies whether the processing of the specified packet is written to the system logs.

Rule 7 states that any traffic coming in on a specified link (Comm_with_Contractor) requesting a Telnet session will be accepted, but logged. This rule also implies that non-Telnet traffic will be denied.



NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Primary_Manage Dallas_Gateway Dallas_InternalW Dallas_Radius	All_Intranet_Gat	* Any	TCP ident NBT UDP bootp	drop	- None	* Policy Targets	* Any	
2	Primary_Manage Dallas_Gateway Dallas_InternalW Dallas_Radius	All_Intranet_Gat	* Any	* Any	drop	Log	* Policy Targets	* Any	
3	Primary_Manage	All_Intranet_Gat	* Any	* Any	drop	Log	* Policy Targets	* Any	
4	* Any	Dallas_network	My_Intranet	MSExchange-20 TCP sqlnet1 sqlnet2 TCP sqlnet2-1521 TCP sqlnet2-1525 TCP sqlnet2-1526	accept	Log	* Policy Targets	* Any	Remote offices workers can connect to the exchange server, read and post emails. ERP is also allowed.
5	* Any	* Any	Dallas_internall_	NBT	accept	- None	* Policy Targets	* Any	Allow the re,pte sites to do anything VPNed with the Dallas ans vice versa.
6	* Any	* Any	My_Intranet	* Any	accept	- None	* Policy Targets	* Any	Don't log NBT connections to the file server.
7	* Any	* Any	Comm_with_Cor	TCP telnet	accept	Log	* Policy Targets	* Any	Support from the contructor is allowed only by telnet.
8	* Any	Dallas_mail1	* Any	smtp->SMTP_Sc	accept	- None	* Policy Targets	* Any	

FIGURE 4-6 Firewall Configuration Rules

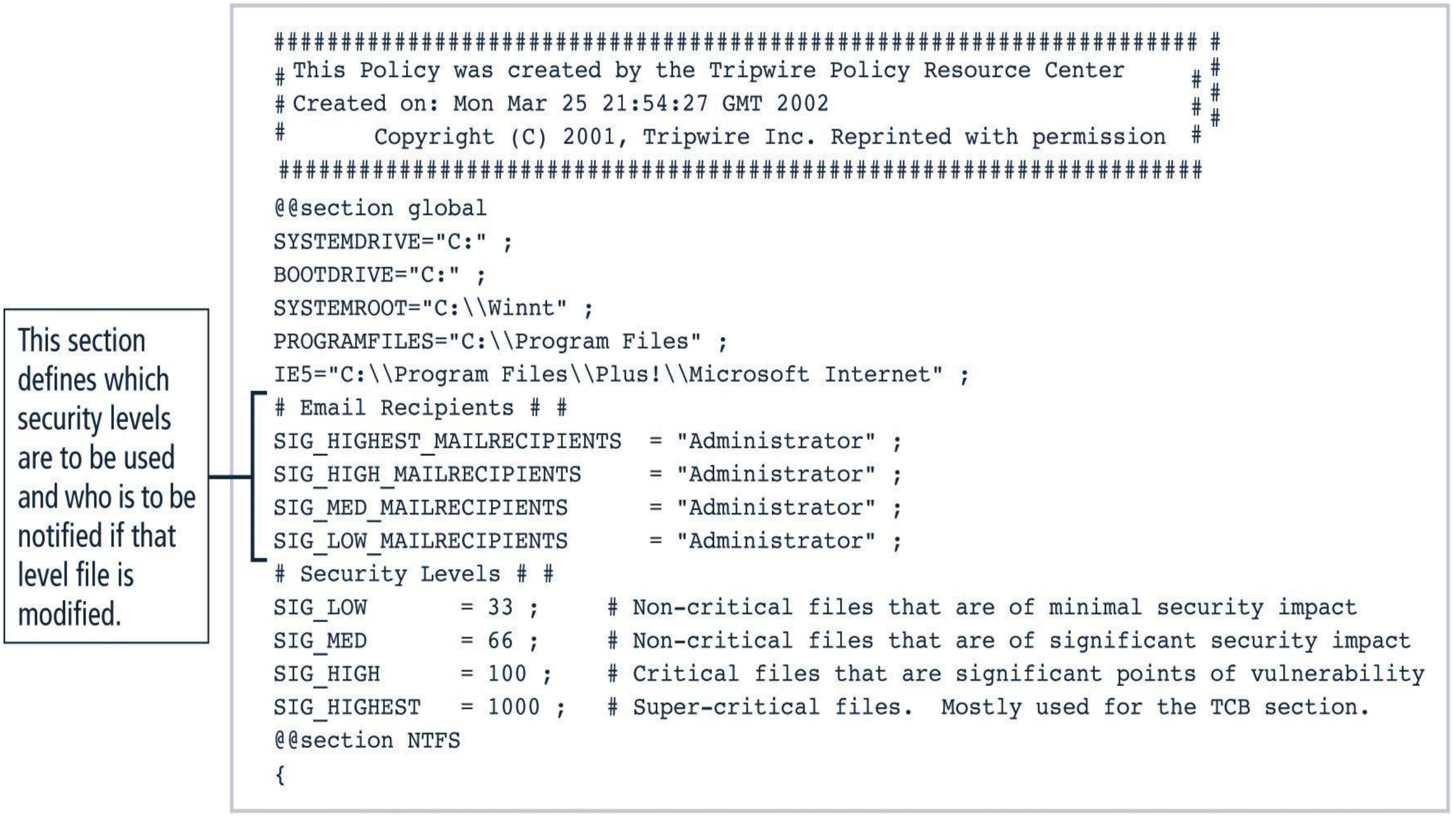
Combination SysSPs

- Often organizations create a single document combining elements of both Management Guidance and Technical Specifications SysSPs

- While this can be confusing, it is very practical

- Care should be taken to articulate required actions carefully as procedures are presented

Figure 4-7
IDS Configuration Rules

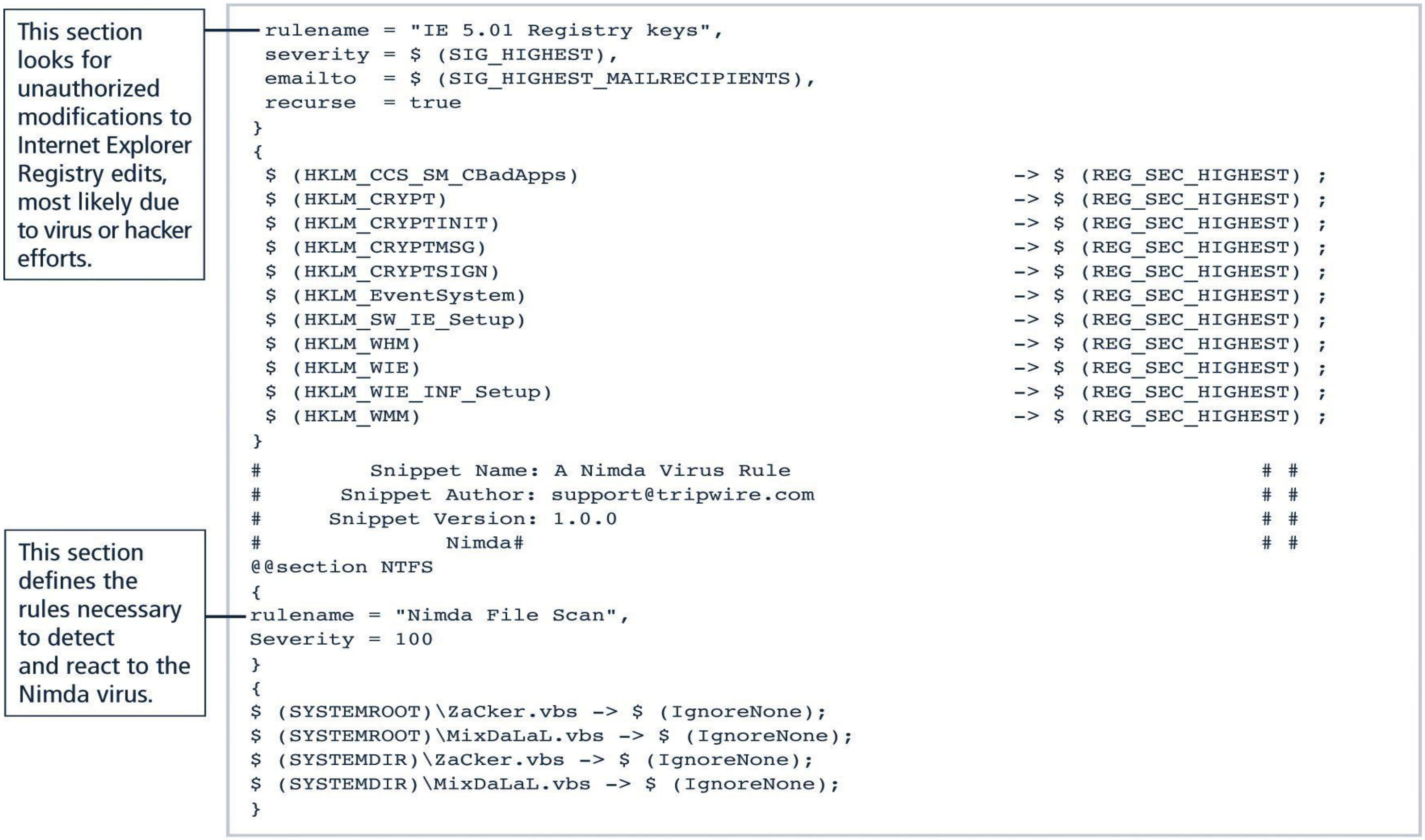


```
##################################################################### #
# This Policy was created by the Tripwire Policy Resource Center     # #
# Created on: Mon Mar 25 21:54:27 GMT 2002                           # #
#       Copyright (C) 2001, Tripwire Inc. Reprinted with permission  # #
#####################################################################
@@section global
SYSTEMDRIVE="C:" ;
BOOTDRIVE="C:" ;
SYSTEMROOT="C:\\Winnt" ;
PROGRAMFILES="C:\\Program Files" ;
IE5="C:\\Program Files\\Plus!\\Microsoft Internet" ;
# Email Recipients # #
SIG_HIGHEST_MAILRECIPIENTS  = "Administrator" ;
SIG_HIGH_MAILRECIPIENTS     = "Administrator" ;
SIG_MED_MAILRECIPIENTS      = "Administrator" ;
SIG_LOW_MAILRECIPIENTS      = "Administrator" ;
# Security Levels # #
SIG_LOW      = 33 ;    # Non-critical files that are of minimal security impact
SIG_MED      = 66 ;    # Non-critical files that are of significant security impact
SIG_HIGH     = 100 ;   # Critical files that are significant points of vulnerability
SIG_HIGHEST  = 1000 ;  # Super-critical files.  Mostly used for the TCB section.
@@section NTFS
{
```

This section defines which security levels are to be used and who is to be notified if that level file is modified.

FIGURE 4-7 IDS Configuration Rules

Figure 4-7
IDS Configuration Rules – (Continued)



This section looks for unauthorized modifications to Internet Explorer Registry edits, most likely due to virus or hacker efforts.

This section defines the rules necessary to detect and react to the Nimda virus.

```
 rulename = "IE 5.01 Registry keys",
 severity = $ (SIG_HIGHEST),
 emailto  = $ (SIG_HIGHEST_MAILRECIPIENTS),
 recurse  = true
}
{
 $ (HKLM_CCS_SM_CBadApps)                                  -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_CRYPT)                                            -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_CRYPTINIT)                                        -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_CRYPTMSG)                                         -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_CRYPTSIGN)                                        -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_EventSystem)                                      -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_SW_IE_Setup)                                      -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_WHM)                                              -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_WIE)                                              -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_WIE_INF_Setup)                                    -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_WMM)                                              -> $ (REG_SEC_HIGHEST) ;
}
#        Snippet Name: A Nimda Virus Rule                                    # #
#      Snippet Author: support@tripwire.com                                  # #
#     Snippet Version: 1.0.0                                                 # #
#              Nimda#                                                        # #
@@section NTFS
{
rulename = "Nimda File Scan",
Severity = 100
}
{
$ (SYSTEMROOT)\ZaCker.vbs -> $ (IgnoreNone);
$ (SYSTEMROOT)\MixDaLaL.vbs -> $ (IgnoreNone);
$ (SYSTEMDIR)\ZaCker.vbs -> $ (IgnoreNone);
$ (SYSTEMDIR)\MixDaLaL.vbs -> $ (IgnoreNone);
}
```

FIGURE 4-7 IDS Configuration Rules (continued)

Guidelines for Policy Development

- Often useful to view policy development as a two-part project
  1. Design and develop policy (or redesign and rewrite outdated policy)
  2. Establish management processes to perpetuate policy within organization
- The former is an exercise in project management, while the latter requires adherence to good business practices

The Policy Project

- Policy development or re-development projects should be well planned, properly funded, and aggressively managed to ensure completion on time and within budget

- When a policy development project is undertaken, the project can be guided by the SecSDLC process

Investigation Phase

- The policy development team should:
  - Obtain support from senior management, and active involvement of IT management, specifically CIO
  - Clearly articulate goals of policy project
  - Gain participation of correct individuals affected by recommended policies
  - Be composed from Legal, Human Resources and end-users
  - Assign project champion with sufficient stature and prestige
  - Acquire a capable project manager
  - Develop detailed outline of and sound estimates for the cost and scheduling of the project

Analysis Phase

- Analysis phase should include the following activities:
  - New or recent risk assessment or IT audit documenting the current information security needs of the organization
  - Key reference materials—including any existing policies

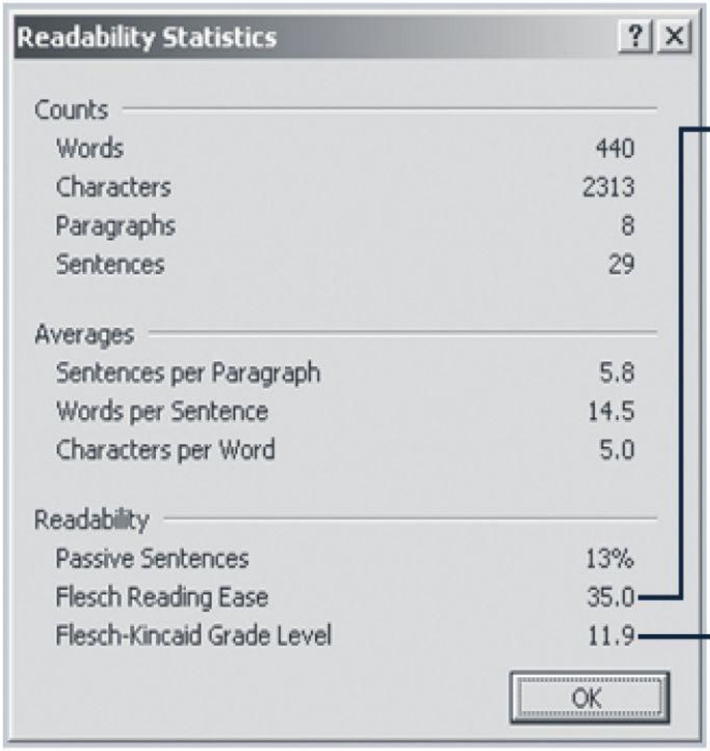
Design Phase

- Design phase should include:
  - How policies will be distributed
  - How verification of distribution will be accomplished
  - Specifications for any automated tools
  - Revisions to feasibility analysis reports based on improved costs and benefits as design is clarified

Implementation Phase

- Implementation Phase: writing the policies
- Make certain policies are enforceable as written
- Policy distribution is not always as straightforward
- Effective policy
  - Is written at a reasonable reading level
  - Attempts to minimize technical jargon and management terminology

Figure 4-9
Readability Statistics Example



Readability Statistics

Counts	
Words	440
Characters	2313
Paragraphs	8
Sentences	29
Averages	
Sentences per Paragraph	5.8
Words per Sentence	14.5
Characters per Word	5.0
Readability	
Passive Sentences	13%
Flesch Reading Ease	35.0
Flesch-Kincaid Grade Level	11.9

The Flesch Reading Ease scale evaluates the writing on a scale of 1 to 100. The higher the score, the easier it is to understand the writing.
This score is too complex for most policies, but appropriate for a college text.
For most corporate documents, a score of 60 to 70 is preferred.

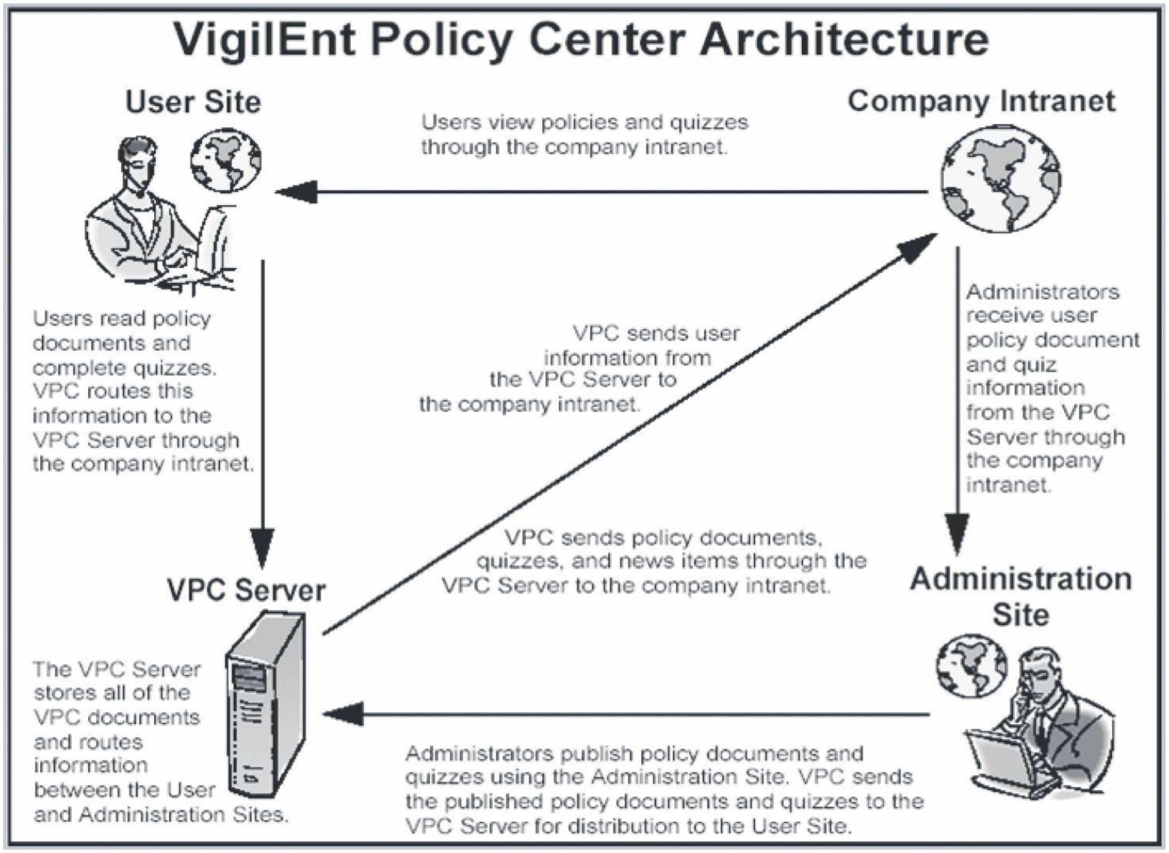
The Flesch-Kincaid Grade Level score evaluates writing on a U.S. grade-school level.
While an eleventh to twelfth grade level may be appropriate for this book, it is too high for an organization's policy.
For most corporate documents, a score of 7.0 to 8.0 is preferred.

FIGURE 4-9 Readability Statistics for Policy

Maintenance Phase

- Maintain and modify policy as needed to ensure that it remains effective as a tool to meet changing threats
- Policy should have a built-in mechanism via which users can report problems with the policy, preferably anonymously
- Periodic review should be built in to the process

Figure 4-10
VigilEnt Policy Center



Users view policies and quizzes through the company intranet.

Users read policy documents and complete quizzes. VPC routes this information to the VPC Server through the company intranet.

VPC sends user information from the VPC Server to the company intranet.

Administrators receive user policy document and quiz information from the VPC Server through the company intranet.

VPC sends policy documents, quizzes, and news items through the VPC Server to the company intranet.

The VPC Server stores all of the VPC documents and routes information between the User and Administration Sites.

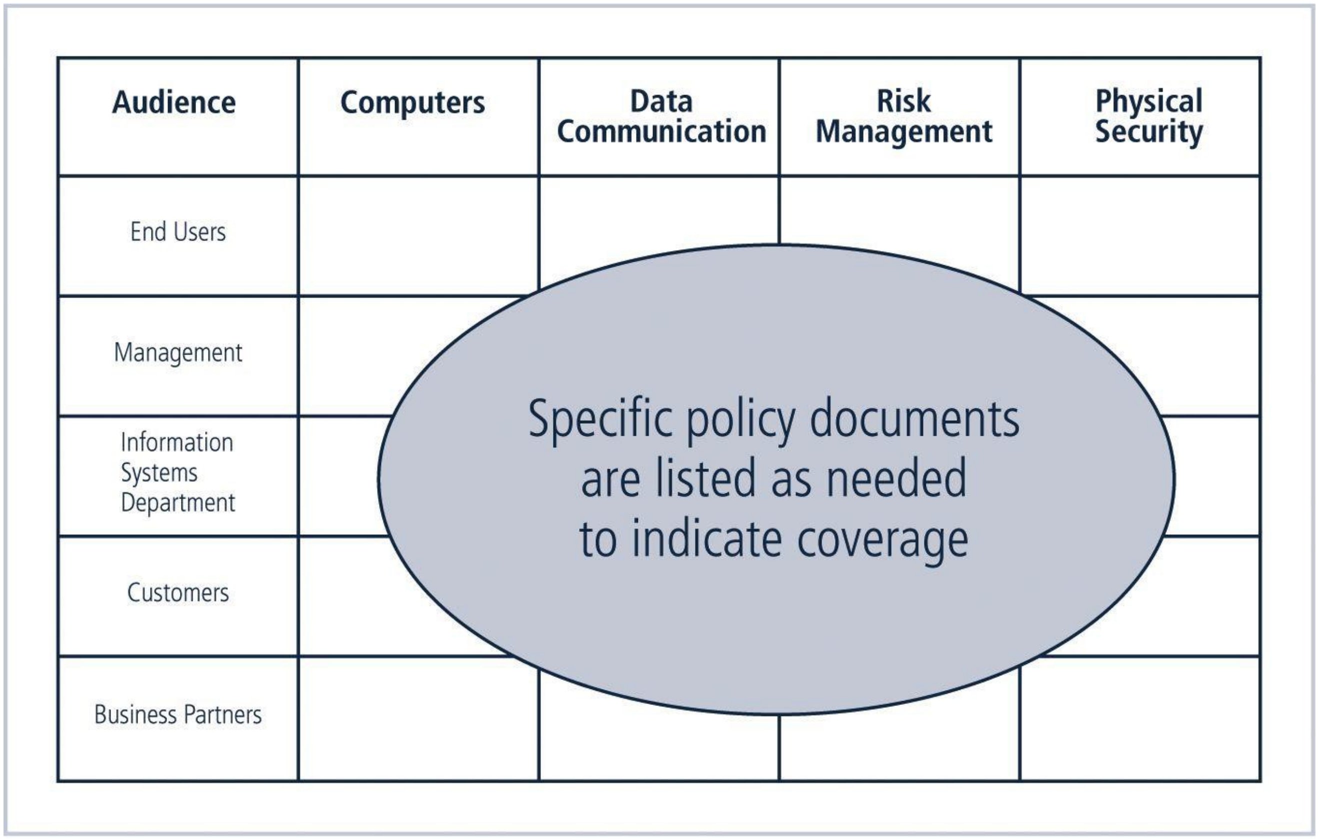
Administrators publish policy documents and quizzes using the Administration Site. VPC sends the published policy documents and quizzes to the VPC Server for distribution to the User Site.

FIGURE 4-10 The VigilEnt Policy Center

The Information Security Policy Made Easy Approach (ISPME)

- Gathering Key Reference Materials
- Defining A Framework For Policies
- Preparing A Coverage Matrix
- Making Critical Systems Design Decisions
- Structuring Review, Approval, And Enforcement Processes

Figure 4-11
Coverage Matrix



Audience	Computers	Data Communication	Risk Management	Physical Security
End Users				
Management				
Information Systems Department				
Customers				
Business Partners				

Specific policy documents are listed as needed to indicate coverage

FIGURE 4-11 A Sample Coverage Matrix

ISPME Checklist

- Perform risk assessment or information technology audit to determine your organization's unique information security needs
- Clarify what “policy” means within your organization so that you are not preparing a “standard,” “procedure,” or some other related material
- Ensure that roles and responsibilities related to information security are clarified, including responsibility for issuing and maintaining policies
- Convince management that it is advisable to have documented information security policies

ISPME Checklist (Continued)

- Identify top management staff who will be approving final information security document and all influential reviewers
- Perform risk assessment or information technology audit to determine organization's unique information security needs
- Clarify what “policy” means within your organization so that you are not preparing a “standard,” “procedure,” or some other related material
- Ensure that roles and responsibilities related to information security are clarified, including responsibility for issuing and maintaining policies

ISPME Checklist (Continued)

- Convince management that it is advisable to have documented information security policies
- Identify top management staff who will be approving final information security document and all influential reviewers
- Collect and read all existing internal information security awareness material and make a list of the included bottom-line messages
- Conduct a brief internal survey to gather ideas that stakeholders believe should be included in a new or updated information security policy

ISPME Checklist (Continued)

- Examine other policies issued by your organization, such as those from Human Resources management, to identify prevailing format, style, tone, length, and cross-references
- Identify audience to receive information security policy materials and determine whether they will each get a separate document or a separate page on an intranet site
- Determine extent to which audience is literate, computer knowledgeable, and receptive to security messages

ISPME Checklist (Continued)

- Decide whether some other awareness efforts must take place before information security policies are issued
- Using ideas from the risk assessment, prepare a list of absolutely essential policy messages that must be communicated
- If there is more than one audience, match the audiences with the bottom-line messages to be communicated through a coverage matrix. […]
- Determine how the policy material will be disseminated, noting the constraints and implications of each medium of communication

ISPME Checklist (Continued)

- Review compliance checking, disciplinary, and enforcement processes to ensure they all can work smoothly with new policy document
- Determine whether number of messages is too large to be handled all at one time, and if so, identify different categories of material that will be issued at different times
- Have an outline of topics to be included in the first document reviewed by several stakeholders
- Based on comments from stakeholders, revise initial outline and prepare a first draft […]

ISPME Checklist (Continued)

- Have first draft document reviewed by stakeholders for initial reactions, presentation suggestions, and implementation ideas
- Revise draft in response to comments from stakeholders
- Request top management approval on policy
- Prepare extracts of policy document for selected purposes
- Develop awareness plan that uses policy document as a source of ideas and requirements

ISPME Checklist (Continued)

- Create working papers memo indicating disposition of all comments received from reviewers, even if no changes were made
- Write memo about project, what you learned, and what needs to be fixed so that next version of policy document can be prepared more efficiently, better received by readers, and more responsive to unique circumstances facing your organization
- Prepare list of next steps that will be required to implement requirements specified in policy document

ISPME Next Steps

- Post Polices To Intranet Or Equivalent
- Develop A Self-Assessment Questionnaire
- Develop Revised user ID Issuance Form
- Develop Agreement To Comply With Information Security Policies Form
- Develop Tests To Determine If Workers Understand Policies
- Assign Information Security Coordinators
- Train Information Security Coordinators

ISPME Next Steps (Continued)

- Prepare And Deliver A Basic Information Security Training Course
- Develop Application Specific Information Security Policies
- Develop A Conceptual Hierarchy Of Information Security Requirements
- Assign Information Ownership And Custodianship
- Establish An Information Security Management Committee
- Develop An Information Security Architecture Document

SP 800-18: Guide for Developing Security Plans

- NIST Special Publication 800-18 offers another approach to policy management
- Policies:
  - Living documents that constantly change and grow
  - Must be properly disseminated (distributed, read, understood and agreed to) and managed

SP 800-18: Guide for Developing Security Plans (Continued)

- Good management practices for policy development and maintenance make for a more resilient organization
- In order to remain current and viable, policies must have:
  - Individual responsible for reviews
  - Schedule of reviews
  - Method for making recommendations for reviews
  - Indication of policy and revision date

A Final Note on Policy

- Lest you believe that the only reason to have policies is to avoid litigation, it is important to emphasize the preventative nature of policy
- Policies exist first, and foremost, to inform employees of what is and is not acceptable behavior in the organization
- Policy seeks to improve employee productivity, and prevent potentially embarrassing situations

Summary

- Introduction
- Why Policy?
- Enterprise Information Security Policy
- Issue-Specific Security Policy
- System-Specific Policy
- Guidelines for Policy Development