Information Security Management

Chapter 4
Information Security Policy

Webster University
Scott Granneman

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

-- Rene Descartes (1596–1650)
“Discours de la Methode”

Upon completion of this chapter,
you should be able to:

Define information security policy
& understand its central role
in a successful infosec program

Know the 3 major types of infosec policy
often used & what goes into each type

Develop, implement, & maintain
various types of infosec policies

This chapter focuses
on infosec policy:

✓ What it is

✓ How to write it

✓ How to implement it

✓ How to maintain it

Policy is an essential foundation
of effective infosec program:

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

more … →

You, the policy maker,
set the tone & the emphasis
on how important a role infosec
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 & regulations,
& assurance of operational continuity,
information integrity, & confidentiality.”

A quality infosec program
begins & ends with policy

Policies are least expensive means of control
& often the most difficult to implement

Basic rules to follow when shaping 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

Focus on the systemic solutions, not specifics

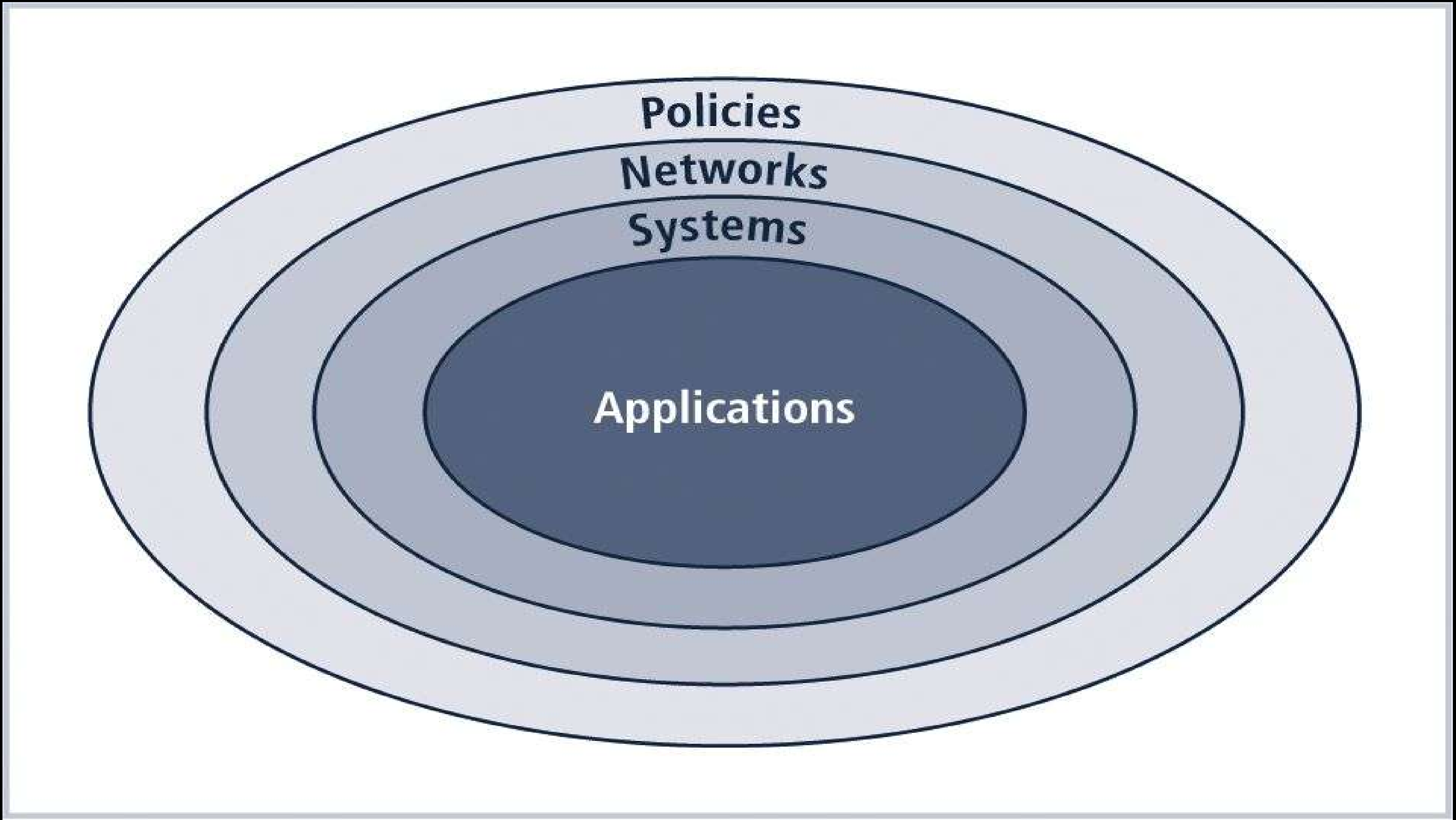


FIGURE 4-1 The Bull's-Eye Model

Bulls-eye model layers:

1. Policies: first layer of defense

2. Networks: threats first meet organization’s network

3. Systems: computers & manufacturing systems

4. Applications: all applications systems

Policies are important reference documents
for internal audits
& for resolution of legal disputes
about management’s due diligence

Policy documents
can act as a clear statement
of management’s intent

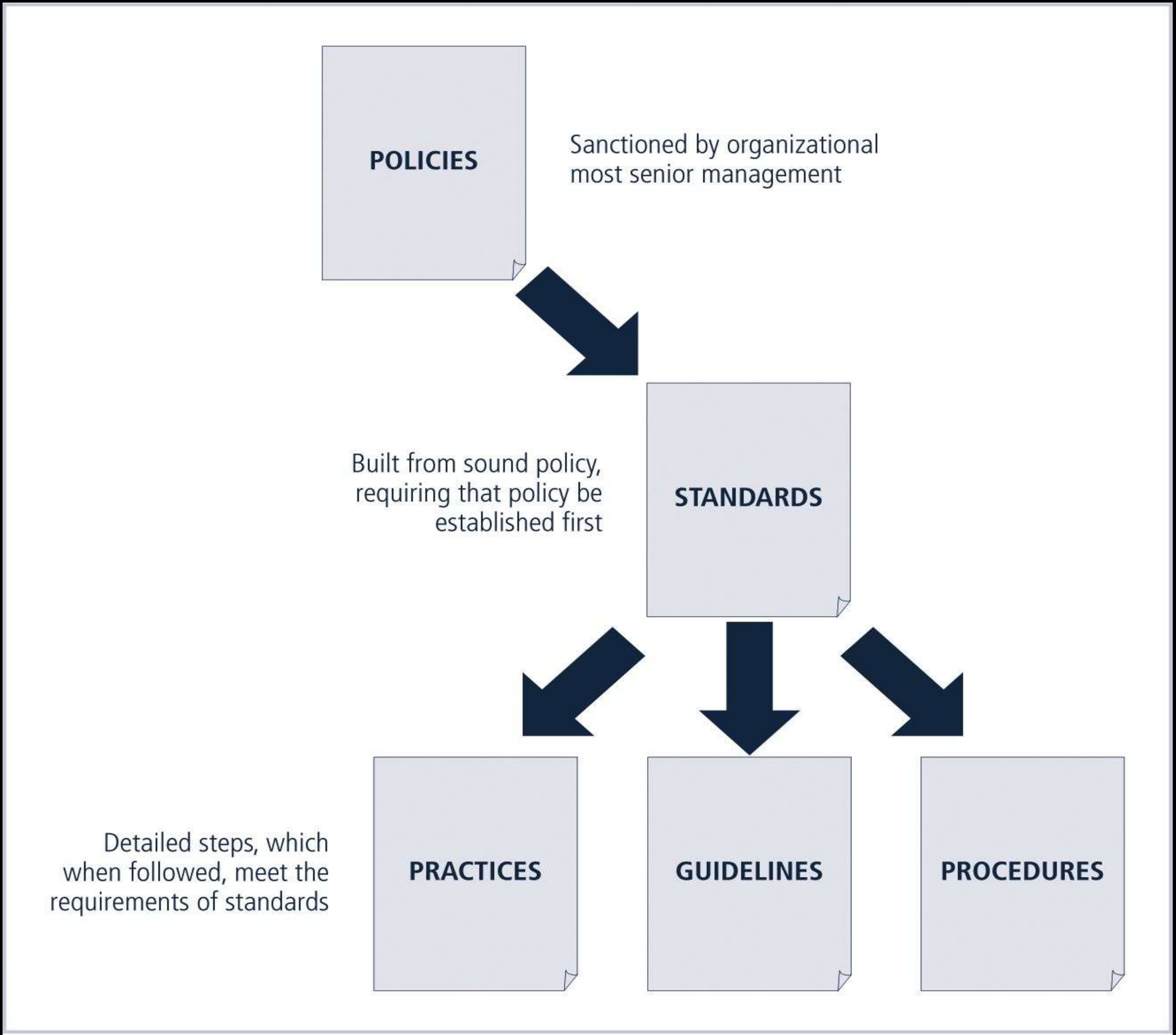

POLICIES
Sanctioned by organizational most senior management
Built from sound policy, requiring that policy be established first
STANDARDS
Detailed steps, which when followed, meet the requirements of standards
PRACTICES
GUIDELINES
PROCEDURES

FIGURE 4-2 Policies, Standards, and Practices

Policy: plan or course of action
that influences & determines decisions

Standards: more detailed statement
of what must be done
to comply with policy

Practices, procedures & guidelines:
explain how employees
will comply with policy

For policies to be effective,
they must be:

✓ Properly disseminated

✓ Read

✓ Understood

✓ Agreed-to

Policies require
constant modification & maintenance

In order to produce
a complete infosec policy,
management must define
3 types of infosec policy:

✓ Enterprise infosec program policy

✓ Issue-specific infosec policies

✓ Systems-specific infosec policies

Enterprise InfoSec Policy (EISP)

✓ Sets strategic direction, scope, & tone
for organization’s security efforts

✓ Assigns responsibilities
for various areas of infosec

✓ Guides development, implementation,
& management requirements
of infosec program

EISP documents should provide:

✓ An overview of
corporate philosophy on security

✓ Information about infosec organization
& infosec roles:

→ Responsibilities for security
shared by all organization members

→ Responsibilities for security
unique to each organizational role

Components of the EISP

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

Sample EISP

Protection Of Information:
Information must be protected
in a manner commensurate
with its sensitivity, value, & criticality

Use Of Information:
Company X information
must be used only for business purposes
expressly authorized by management

Information Handling, Access, & Usage:
Information is a vital asset
& all accesses to, uses of, & processing of
Company X information
must be consistent with policies & standards

more ... →

Data & 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, & availability
of the information handled by computers
& communications systems

Legal Conflicts:
Company X infosec policies were drafted
to meet or exceed the protections found
in existing laws & regulations,
& any Company X infosec policy
believed to be in conflict
with existing laws or regulations
must be promptly reported to infosec management

more … →

Exceptions To Policies:
Exceptions to infosec 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,
& where this form has been approved
by both InfoSec management
& Internal Audit management

Policy Non-Enforcement:
Management's non-enforcement
of any policy requirement
does not constitute its consent

more … →

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 InfoSec Standards:
Company X information systems
must employ industry-specific infosec standards

more … →

Use Of infosec Policies & Procedures:
All Company X infosec documentation
including, but not limited to,
policies, standards, & 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 tech systems

✓ Begins with intro to fundamental
technological philosophy of organization

✓ Serves to protect employee & organization
from inefficiency/ambiguity

✓ Documents how technology-based system
is controlled

✓ Identifies processes & authorities
that provide this control

✓ Serves to indemnify organization against liability
for inappropriate or illegal system use

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:

✓ email

✓ use of Internet & World Wide Web

✓ specific minimum configurations of computers
to defend against malware

✓ 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 & Applicability
✓ Definition of Technology Addressed
✓ Responsibilities

Authorized Access & Usage of Equipment:

✓ User Access
✓ Fair & Responsible Use
✓ Protection of Privacy

more … →

Prohibited Usage of Equipment:

✓ Disruptive Use or Misuse
✓ Criminal Use
✓ Offensive or Harassing Materials
✓ Copyrighted, Licensed, or other Intellectual Property
✓ Other Restrictions

Systems Management:

✓ Management of Stored Materials
✓ Employer Monitoring
✓ Virus Protection
✓ Physical Security
✓ Encryption

more … →

Violations of Policy:

✓ Procedures for Reporting Violations
✓ Penalties for Violations

Policy Review & Modification:

✓ Scheduled Review of Policy
& Procedures for Modification

Limitations of Liability:

✓ Statements of Liability or Disclaimers

Common approaches
to implementing ISSP:

✓ Number of independent ISSP documents

✓ Single comprehensive ISSP document

✓ Modular ISSP document
that unifies policy creation & administration

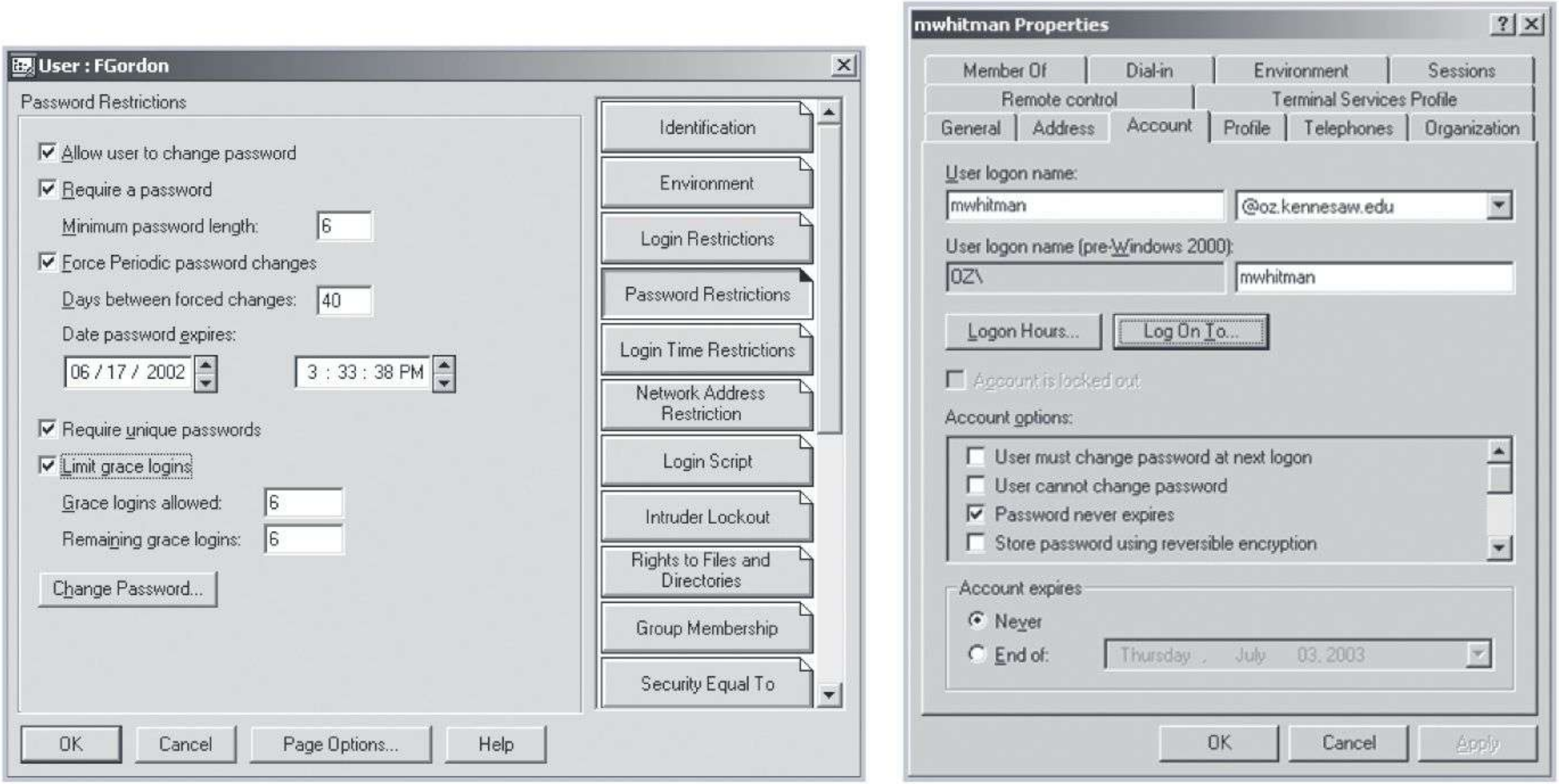
Recommended approach is modular policy,
which provides a balance between
issue orientation & policy management

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



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 & 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:

1. Access control lists
2. Configuration rules

Access Control Lists

ACLs enable administrations to restrict access according to user, computer, time, duration, or even a particular file

more … →

Include user access lists, matrices,
& capability tables that govern rights & privileges

Can control access to file storage systems,
object brokers,
or other network communications devices

Capability Table:
similar method that specifies
which subjects & objects
users or groups can access

Specifications are frequently complex matrices,
rather than simple lists or tables

Level of detail & specificity
(often called granularity)
may vary from system to system

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, & applications

ACL Administrators set user privileges, such as:

✓ Read
✓ Write
✓ Create
✓ Modify
✓ Delete
✓ Compare
✓ Copy

Configuration rules
are specific configuration codes
entered into security systems
to guide execution of system
when information is passing through it

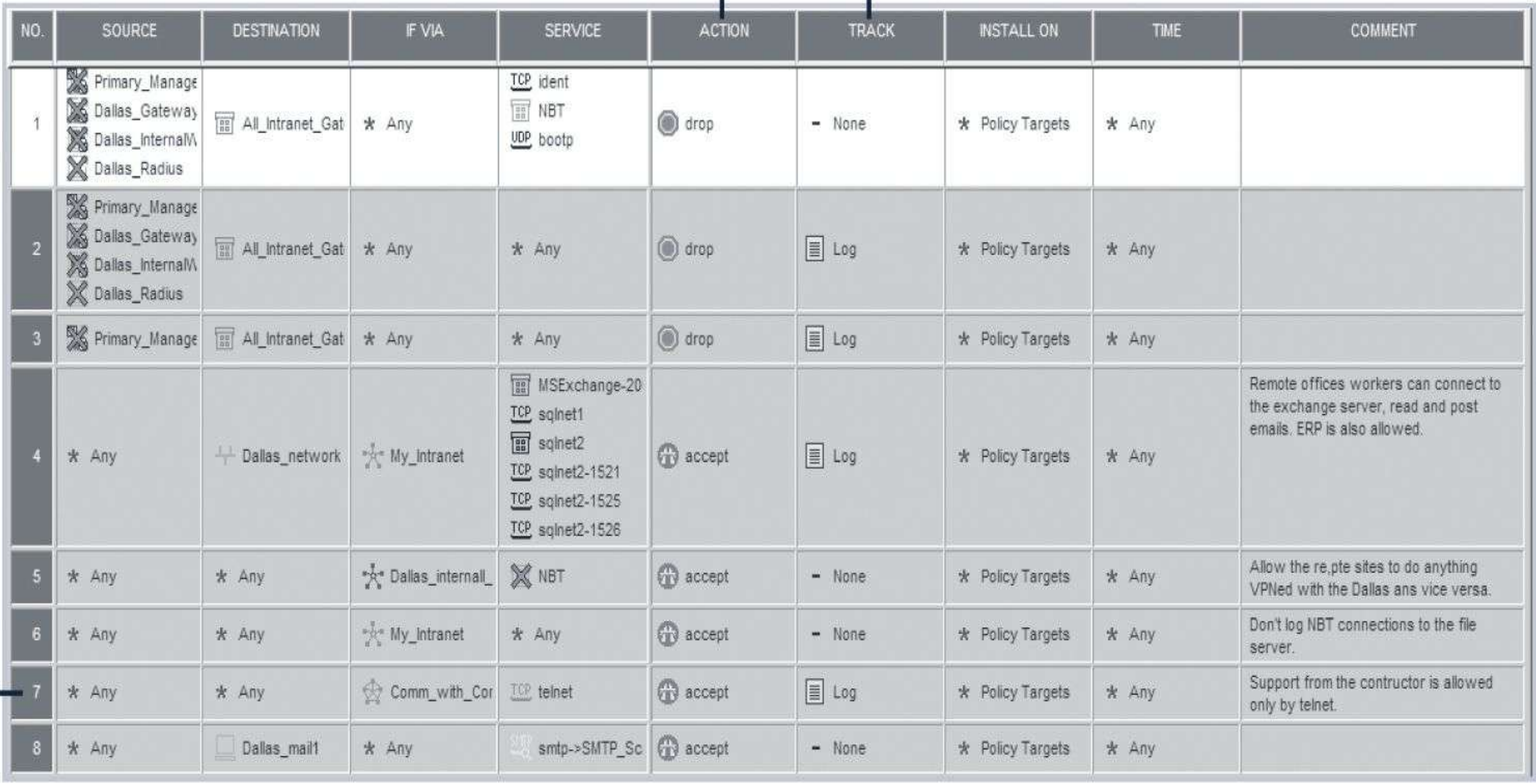
Rule policies are more specific
to system operation than ACLs
& may or may not deal with users directly

Many security systems
require specific configuration scripts
telling systems what actions to perform
on each set of information processed

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_InternalM Dallas_Radius	All_Intranet_Gat	* Any	TCP ident NBT UDP bootp	drop	- None	* Policy Targets	* Any	
2	Primary_Manage Dallas_Gateway Dallas_InternalM 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	

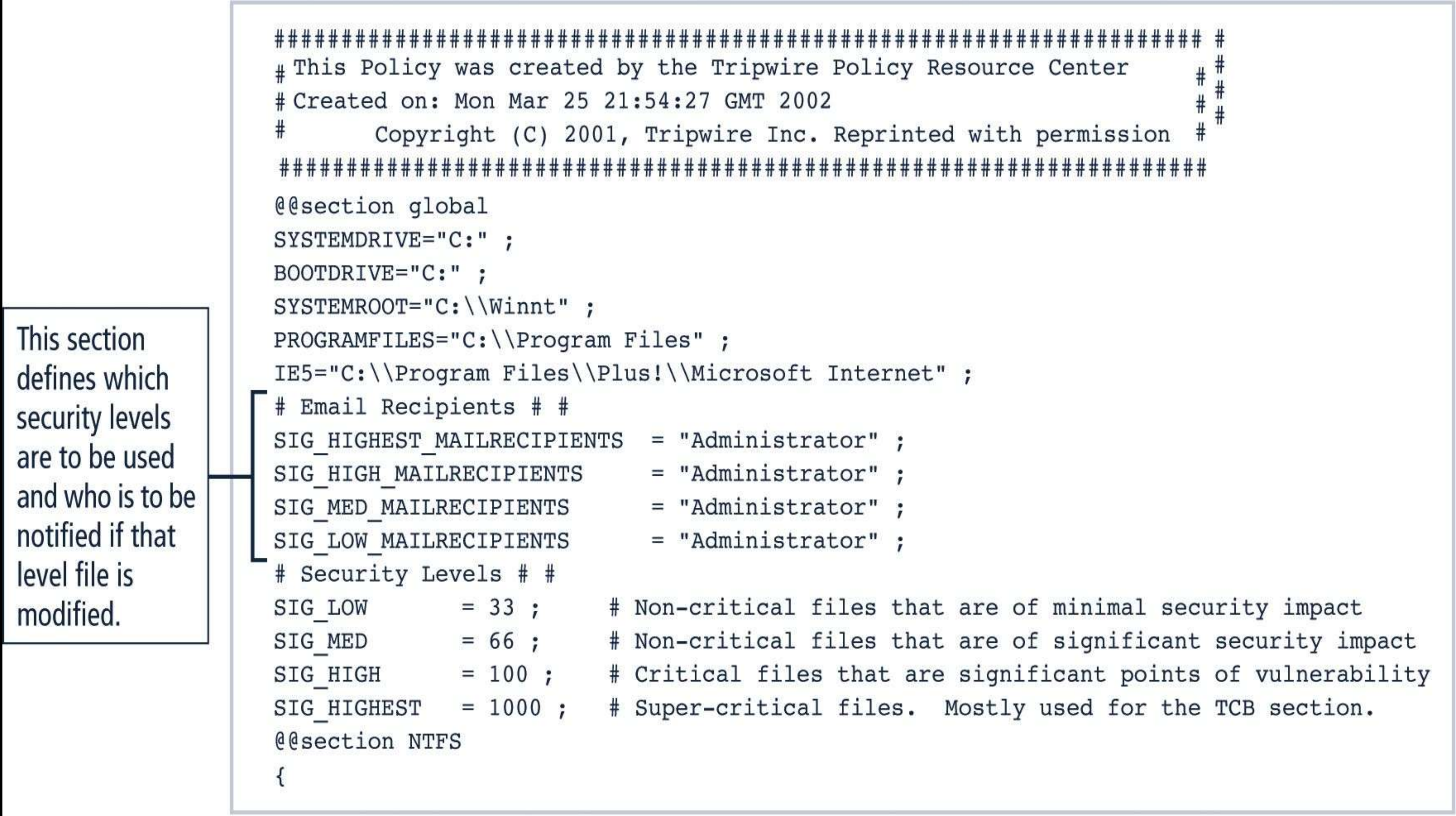
FIGURE 4-6 Firewall Configuration Rules

Combination SysSPs

✓ Often organizations create
a single document
combining elements of both
Management Guidance
& Technical Specifications SysSPs

✓ While this can be confusing,
it is very practical

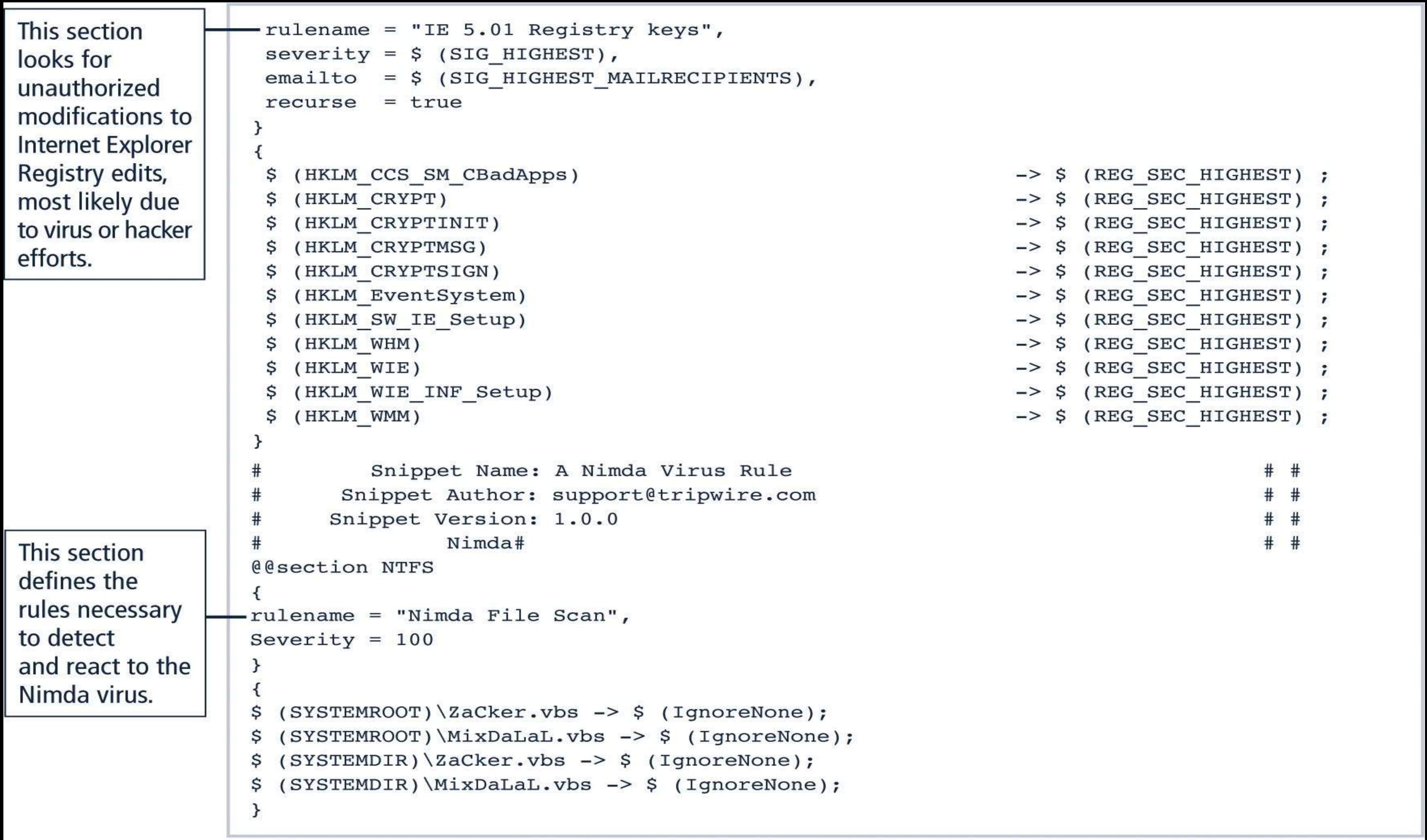
✓ Care should be taken
to articulate required actions carefully
as procedures are presented



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

```
#################################################################### #
# 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
{
```

FIGURE 4-7 IDS Configuration Rules



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

```
 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);
}
```

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

FIGURE 4-7 IDS Configuration Rules (continued)

Guidelines for Policy Development

Often useful to view policy development
as a two-part project:

1. Design & develop policy
(or redesign & 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

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

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

1. Investigation Phase

The policy development team should:

✓ Obtain support from senior management,
& active involvement of IT management,
specifically CIO

✓ Clearly articulate goals of policy project

✓ Gain participation
of correct individuals
affected by recommended policies

more … →

✓ Be composed from
Legal, Human Resources & end-users

✓ Assign project champion
with sufficient stature & prestige

✓ Acquire a capable project manager

✓ Develop detailed outline of
& sound estimates for,
the cost & scheduling of the project

2. Analysis Phase

Should include the following activities:

✓ New or recent
risk assessment or IT audit
documenting the current infosec needs
of the organization

✓ Key reference materials,
including any existing policies

3 & 4. 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 & benefits as design is clarified

5. Implementation Phase

Write the policies!

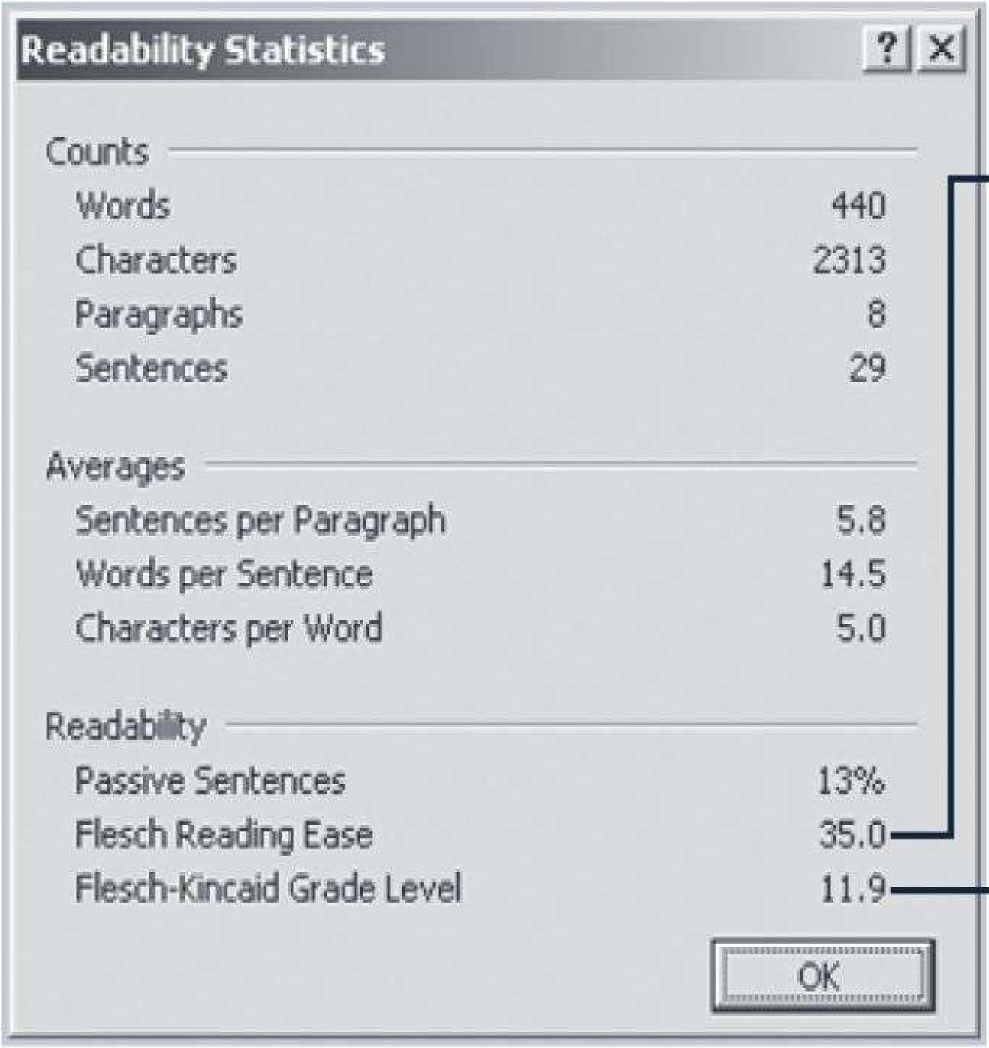
Make certain policies are enforceable as written

Policy distribution is not always as straightforward

Effective policy:

✓ Is written at a reasonable reading level
✓ Attempts to minimize technical jargon & management terminology

One way to measure readability



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.

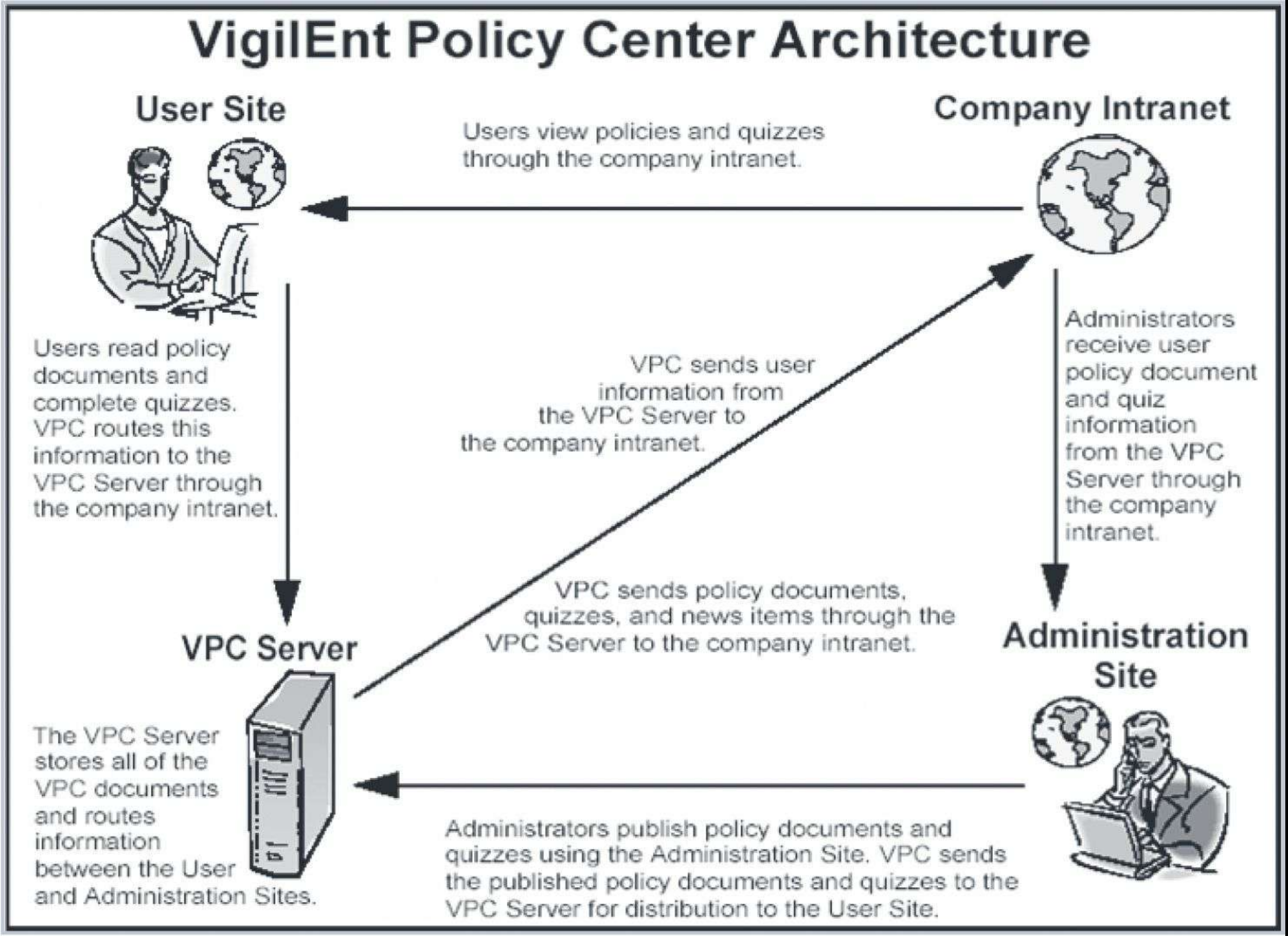
FIGURE 4-9 Readability Statistics for Policy

6. Maintenance Phase

Maintain & 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 into the process



VigilEnt Policy Center Architecture

User Site

Company Intranet

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.

VPC Server

Administration Site

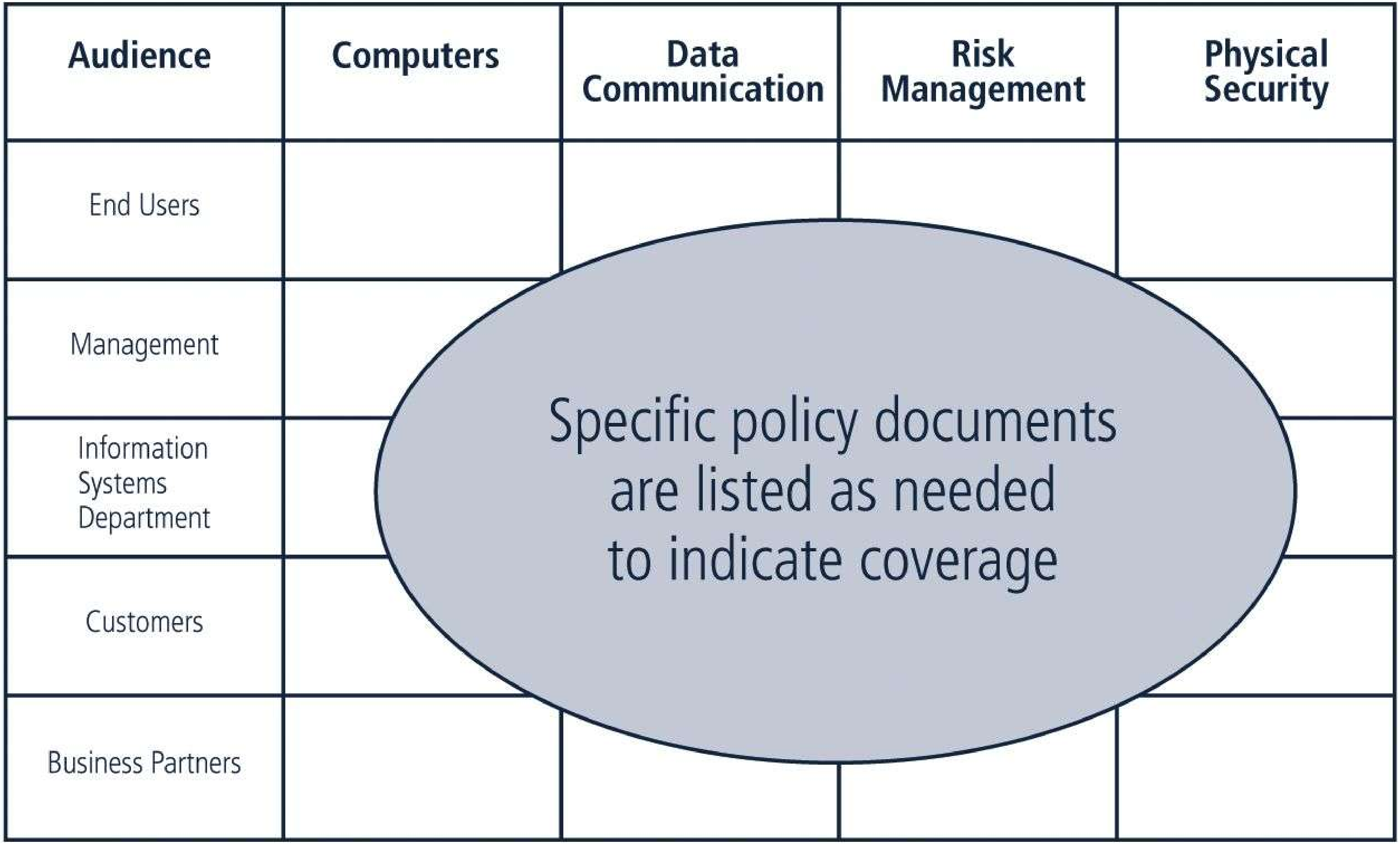
The VPC Server stores all of the VPC documents and routes information between the User and Administration Sites.

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 InfoSec 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, & Enforcement Processes



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 org’s unique infosec needs

✓ Clarify what “policy” means
within your org so that you are not preparing
a “standard,” “procedure,”
or some other related material

✓ Ensure that roles & responsibilities
related to infosec are clarified,
including responsibility
for issuing & maintaining policies

more … →

✓ Convince management that it is advisable
to have documented infosec policies

✓ Identify top management staff
who will be approving final infosec document
& all influential reviewers

✓ Collect & read
all existing internal infosec awareness material
& 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 infosec policy

more … →

✓ Examine other policies
issued by your organization,
such as those from HR management,
to identify prevailing
format, style, tone, length, & cross-references

✓ Identify audience to receive infosec policy materials
& 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,
& receptive to security messages

more … →

✓ Decide whether some other awareness efforts must take place before infosec 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.

more ... →

✓ Determine how the policy material
will be disseminated,
noting the constraints & implications
of each medium of communication

✓ Review compliance checking, disciplinary,
& 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,
& if so,
identify different categories of material
that will be issued at different times

more … →

✓ Have an outline of topics to be included
in the first document
reviewed by several stakeholders

✓ Based on comments from stakeholders,
revise initial outline & prepare a first draft

✓ Have first draft document
reviewed by stakeholders
for initial reactions, presentation suggestions,
& implementation ideas

✓ Revise draft
in response to comments from stakeholders

more … →

✓ 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 & requirements

✓ Create working papers memo
indicating disposition of all comments
received from reviewers,
even if no changes were made

more … →

✓ Write memo about project, what you learned,
& what needs to be fixed
so that next version of policy document
can be prepared more efficiently,
better received by readers,
& 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 InfoSec Policies Form

✓ Develop Tests To Determine
If Workers Understand Policies

✓ Assign InfoSec Coordinators

✓ Train InfoSec Coordinators

more ... →

✓ Prepare & Deliver A Basic InfoSec Training Course

✓ Develop Application Specific InfoSec Policies

✓ Develop A Conceptual Hierarchy
Of InfoSec Requirements

✓ Assign Information Ownership & Custodianship

✓ Establish An infosec Management Committee

✓ Develop An infosec Architecture Document

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 & foremost
to inform employees of
what is & is not acceptable behavior
in the organization

Policy seeks to improve employee productivity,
& prevent potentially embarrassing situations

Summary

Why Policy?

Enterprise InfoSec Policy

Issue-Specific Security Policy

System-Specific Policy

Guidelines for Policy Development

Thank you!

Scott Granneman