Management of Information Security, 4th Edition

Chapter 4

Information Security Policy

Objectives

- Define information security policy and understand its central role in a successful information security program
- Describe the three major types of information security policy and discuss the major components of each
- Discuss the process of developing, implementing, and maintaining, various types of information security policies

Why Policy? Part 1

- **Information security policies**: written instructions to inform employees and others in the workplace of the proper behavior regarding use of information and information assets
  - Provided by management
- The policy is designed to:
  - Provide structure in the workplace and explain the will of the of the organization
  - Create a productive and effective work environment

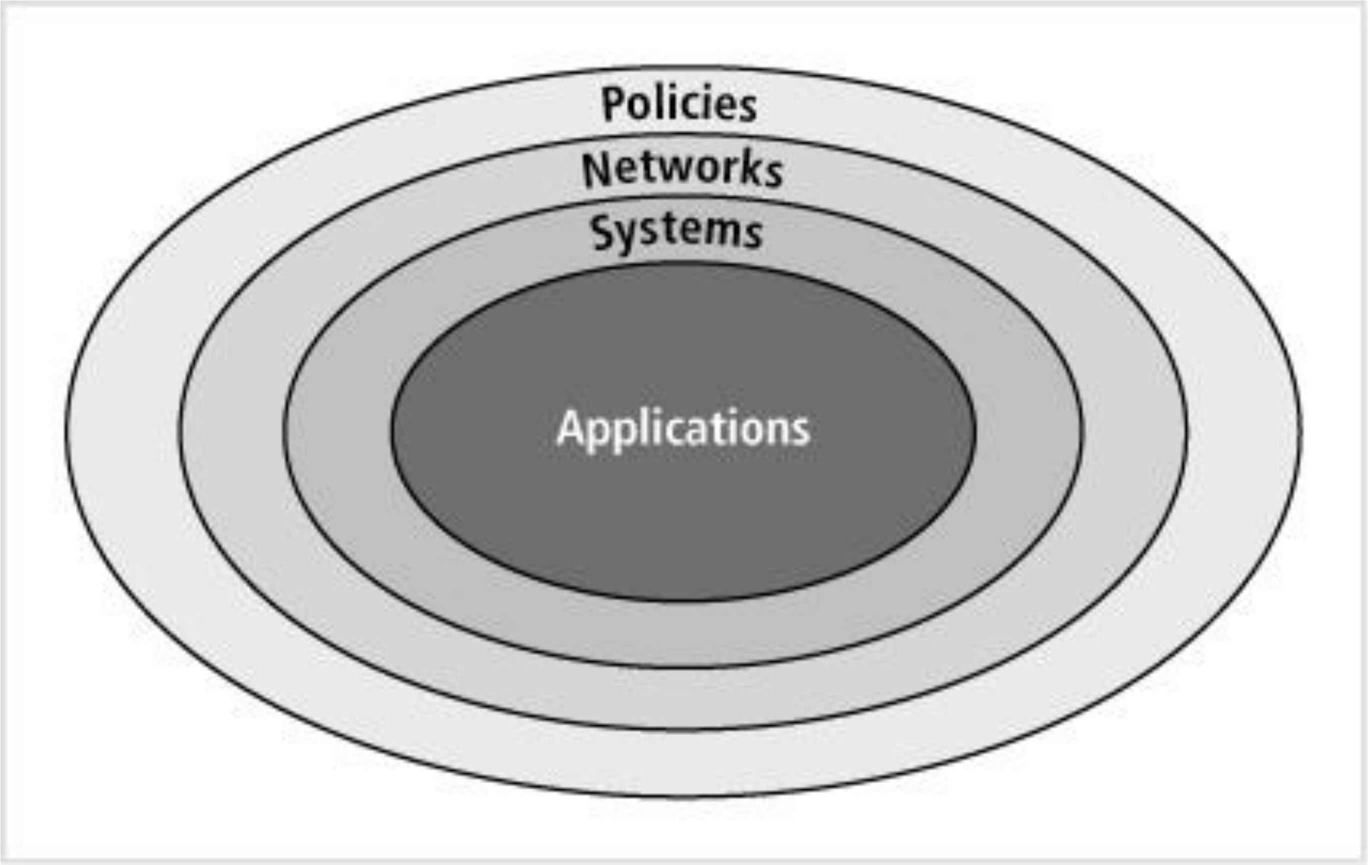
Why Policy? Part 2

- Basic rules to follow when shaping a policy:
  - Policy should never conflict with law
  - Policy must be able to stand up in court if challenged
  - Policy must be properly supported and administered
- Guidelines when creating the IT and InfoSec policy:
  - All polices must contribute to the success of the organization
  - Management must ensure adequate sharing of responsibility for proper use of information systems
  - End users of information systems should be involved in the steps of policy formulation

Why Policy? Part 3

- Bull’s-eye model: provides a mechanism for prioritizing complex changes

Figure 4-1 Bull's-eye model



Policy, Standards, and Practices Part 1

- **Policy**: a plan or course of action intended to influence and determine decisions, actions, and other matters
- Policies direct how issues should be addressed and technologies should be used
- Policies should not specify the proper operation of equipment or software
  - This should be placed in other documentation called standards, procedures, practices, and guidelines

Policy, Standards, and Practices Part 2

- **Standard**: a detailed statement of what must be done to comply with policy
- **Practices, procedures, and guidelines**: explain how employees are to comply with policy

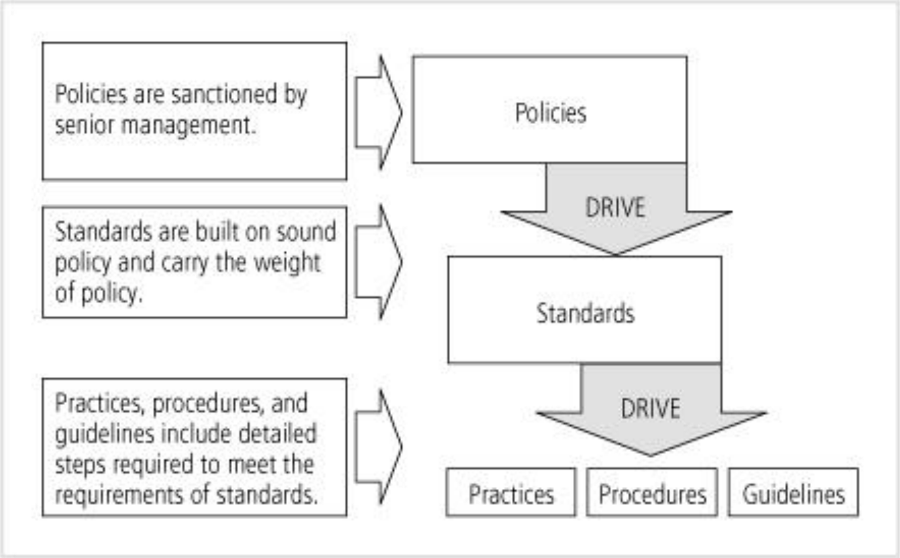

Policies are sanctioned by senior management.
Standards are built on sound policy and carry the weight of policy.
Practices, procedures, and guidelines include detailed steps required to meet the requirements of standards.
Policies
DRIVE
Standards
DRIVE
Practices
Procedures
Guidelines

Figure 4-2 Policies, standards, and practices

Policy, Standards, and Practices Part 3

- To produce a complete InfoSec policy, management must define three types of InfoSec policies:
  - Enterprise information security policy (EISP)
  - Issue-specific security policies (ISSP)
  - System-specific security policies (SysSP)
- Usual procedure is to create the EISP first
  - The highest level of policy

Enterprise Information Security Policy

- Enterprise information security policy (EISP) - sets the strategic direction, scope, and tone for all of an organization's security efforts
- EISP is also known as:
  - Security program policy
  - General security policy
  - IT security policy
  - High-level InfoSec policy or simply "InfoSec policy"
- EISP must directly support the organization's vision and mission statements

Integrating an Organization’s Mission and Objectives into the EISP

- The EISP should state the importance of InfoSec to the organization’s mission and objectives
- InfoSec strategic planning derives from other organizational strategic policies, such as:
  - IT strategic policy
  - Key business unit strategic policies
- The EISP should not contradict the organizational mission statement

EISP Elements

- EISP documents should include the following:
  - An overview of the corporate philosophy on security
  - Information on the structure of InfoSec and individuals who fulfill the InfoSec role
  - Fully articulated responsibilities for security that are shared by all members of the organization
  - Fully articulated responsibilities for security that are unique to each role within the organization

Table 4-1 Components of the EISP

Component	Description
Purpose	Answers the question "What is this policy for?" Provides a framework that helps the reader understand the intent of the document. Can include text such as the following, which is taken from Washington University at St. Louis: "This document will: • Identify the elements of a good security policy • Explain the need for information security • Specify the various categories of information security • Identify the information security responsibilities and roles • Identify appropriate levels of security through standards and guidelines This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs."*
Elements	Defines the whole topic of information security within the organization as well as its critical components. For example, the policy may state: "Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology" and then identify where and how the elements are used. This section can also lay out security definitions or philosophies to clarify the policy.
Need	Justifies the need for the organization to have a program for information security. This is done by providing information on the importance of InfoSec in the organization and the obligation (legal and ethical) to protect critical information, whether regarding customers, employees, or markets.
Roles and responsibilities	Defines the staffing structure designed to support InfoSec within the organization. It will likely describe the placement of the governance elements for InfoSec as well as the categories of individuals with responsibility for InfoSec (IT department, management, users) and their InfoSec responsibilities, including maintenance of this document.
Reference to other policies, standards, and guidelines	Lists other standards that influence and are influenced by this policy document, perhaps including relevant laws (federal and state) and other policies.

Issue-Specific Security Policy Part 1

- **Issue-specific security policy (ISSP)** - provides detailed, targeted guidance to instruct all members of the organization in the use of a resource
- An effective ISSP accomplishes the following:
  - Articulates the organization’s expectations about how its technology-based system should be used

Issue-Specific Security Policy Part 2

- Areas for which an ISSP may be used:
  - Use of e-mails, instant messaging (IM), and other electronic communications applications
  - Use of the Internet on company and personal time
  - Malware protection requirements
  - Installation and use of nonorganizationally issued software or hardware
  - Prohibitions against hacking or testing the organization’s security controls
  - Home use of company-owned computer equipment or removal of equipment from organizational property

Issue-Specific Security Policy Part 3

- Areas for which an ISSP may be used (cont'd):
  - Use of personal equipment on company networks
  - Use of telecommunications technologies (fax, phone, mobile phone)
  - Use of photocopying and scanning equipment

Components of the ISSP

- **Statement of purpose** - the ISSP should begin with a clear statement of purpose that outlines the scope and applicability of the policy
- **Authorized Uses** - explains who can use the technology governed by the policy and for what purposes
- **Prohibited Uses** - this section outlines what the issue or technology cannot be used for

Components of the ISSP (continued)

- **Systems Management** - focuses on the users' relationships to systems management
- **Violations of Policy** - specifies the penalties of violating the usage and systems management policies
- **Policy Review and Modification** - outlines a specific methodology for the review and modification of the ISSP
- **Limitation of Liability** - offers a general statement of liability or a set of disclaimers

Table 4-4 ISSP Document organization approaches

Approach	Advantages	Disadvantages
Individual policy	• Clear assignment to a responsible department • Written by those with superior subject matter expertise for technology-specific systems	• Typically yields a scattershot result that fails to cover all of the necessary issues • Can suffer from poor policy dissemination, enforcement and review
Comprehensive policy	• Well controlled by centrally managed procedures, assuring complete topic coverage • Often provides better formal procedures than when policies are individually formulated • Usually identifies processes for dissemination, enforcement, and review	• May overgeneralize the issues and skip over vulnerabilities • May be written by those with less complete subject matter expertise
Modular policy	• Often considered an optimal balance between the individual ISSP and the comprehensive ISSP approaches • Well controlled by centrally managed procedures, assuring complete topic coverage • Clear assignment to a responsible department • Written by those with superior subject matter expertise for technology-specific systems	• May be more expensive than other alternatives • Implementation can be difficult to manage

System-Specific Security Policy

- System-specific security policies (SysSPs) - often function as standards or procedures to be used when configuring or maintaining systems
  - Example: to configure and operate a network firewall
- SysSPs can be separated into two general groups
  - Managerial guidance
  - Technical specifications

Managerial Guidance SysSPs

- A managerial guidance SysSP document is created by management
  - To guide the implementation and configuration of technology
  - As well as to address the behavior of employees in ways that support the security of information
- Any technology that affects the confidentiality, integrity, or availability of information may require SysSPs
- SysSPs can be developed at the same time as ISSPs

Technical Specification SysSPs

- A systems administrator may need to create a policy to implement a managerial policy
- Example: an ISSP may require that user passwords be changed quarterly
  - A systems administrator can implement a technical control within a specific application to enforce this policy
- Two general methods of implementing technical controls:
  - Access control lists and configuration rules

Access Control Lists

- Access control lists (ACLs) - can control access to file storage systems, object brokers, or other network communications devices
- A capability table specifies which subjects and objects that users or groups can access
  - Also known as “user profiles” or “user policies”
- In general, ACLs enable administrators to restrict access according to:
  - User, computer, time, duration, or even a particular file

Access Control Lists (continued)

- In general, ACLs regulate the following:
  - 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
- To restrict what users can access administrators assign users privileges such as:
  - Read, Write, Execute, or Delete

Combination SysSPs

- Many organizations create a single document that combines elements of the:
  - Management guidance SysSP
  - Technical specifications SysSP

Guidelines for Effective Policy

- Policy is only enforceable if it is properly designed, developed, and implemented using a process that assures repeatable results
- For policies to be effective, they must be properly:
  - Developed using industry-accepted practices
  - Distributed using all appropriate methods
  - Read by all employees
  - Understood by all employees
  - Formally agreed to by act or affirmation
  - Uniformly applied and enforced

Developing Information Security Policy

- It is often useful to view policy development as a two-part project:
  - First, policy is designed and developed (or, redesigned and rewritten, if policy is outdated)
  - Next, management processes are established to perpetuate the policy within the organization
- Policy development should be well planned, properly funded, and aggressively managed
  - To ensure it is completed on time and within budget
- To accomplish this goal, use a systems development life cycle (SDCL)

Investigation Phase

- During the investigation phase, the policy development team should attain:
  - Support from senior management
  - Support and active involvement of IT management
  - Clear articulation of goals
  - Participation of the correct individuals from the communities of interest affected by the policies
  - A detailed outline of the scope of the policy development project
    - As well as sound estimates for cost and scheduling of the project

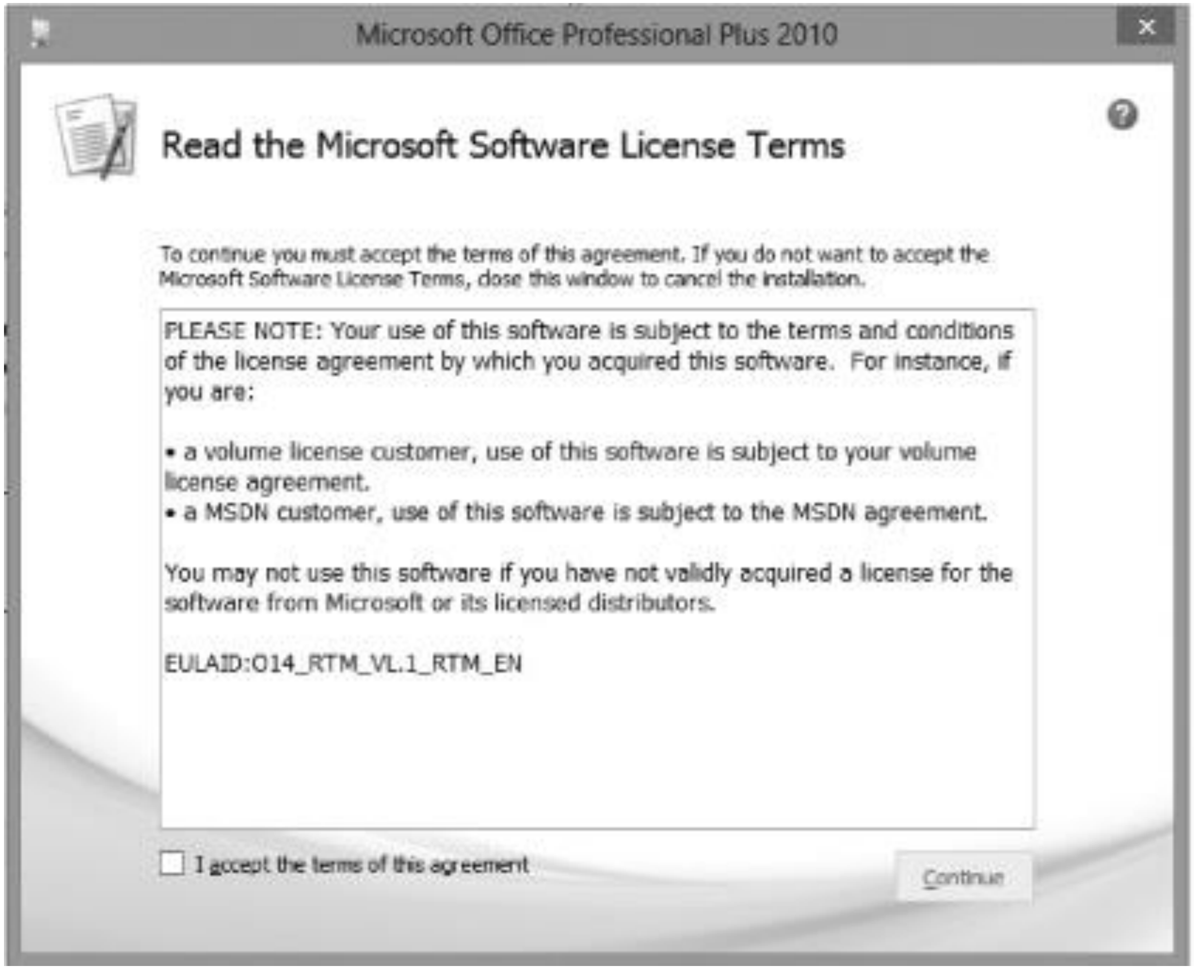
Analysis Phase

- The analysis phase should produce the following:
  - A new or recent risk assessment or IT audit documenting the current InfoSec needs
  - The gathering of key reference materials, including any existing policies
    - Policy documents may be housed in human resources, accounting, finance, legal, or corporate security departments

Design Phase

- During the design phase:
  - The team must create a plan to distribute and verify the distribution of the policies
- Members of the organization must explicitly acknowledge that they have received and read the policy
- Companies may use banners or pop-up windows to display end-user license agreements (EULAs)
  - Spells out responsible use of the software

Figure 4-8 End-user license agreement



Read the Microsoft Software License Terms

To continue you must accept the terms of this agreement. If you do not want to accept the Microsoft Software License Terms, close this window to cancel the installation.

PLEASE NOTE: Your use of this software is subject to the terms and conditions of the license agreement by which you acquired this software. For instance, if you are:

• a volume license customer, use of this software is subject to your volume license agreement.
• a MSDN customer, use of this software is subject to the MSDN agreement.

You may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors.

EULAID:O14_RTM_VL.1_RTM_EN

□ I accept the terms of this agreement

Source: Microsoft.

Implementation Phase

- In the implementation phase, the team:
  - Writes the policies
  - Ensures the policy is prepared correctly, distributed, read, understood, and agreed to by those to whom it applies
- Resources include:
  - The Web
  - Government sites
  - Professional literature
  - Peer networks
  - Professional consultants

Maintenance Phase

- During the maintenance phase, the policy development team:
  - Monitors, maintains, and modifies the policy as needed to ensure it remains effective as a tool to meet changing threats
- The policy should have a built-in mechanism through which users can report problems

Policy Distribution

- Most common methods of policy distribution:
  - Hard copy distribution
  - Electronic distribution
- Unless the organization can prove that the policy actually reached the end users, it cannot be enforced
- Distribution of classified policies (containing confidential internal information)
  - Requires additional levels of controls

Policy Distribution (continued)

- E-mail distribution advantages and disadvantages:
  - Easy to send a document and track when the employee opens the e-mail
  - Becomes cumbersome for employee’s to review inapplicable policies and can quickly fill the e-mail application’s storage capacity
- Best method is electronic policy distribution software

Policy Reading

- Literacy or language issues can be a barrier to an employee’s reading of policies
  - Many jobs do not require literacy skills
- Multinational organizations must deal with challenges of gauging reading levels of foreign citizens
- Translation issues have created challenges for organizations

Policy Comprehension

- To be certain that employees understand the policy
  - The document must be written at a reasonable reading level

- Quizzes and other examinations can be employed to assess which employees understand the policy

Policy Compliance

- Policy compliance is when an employee agrees to the policy
- Failure to agree to a policy is tantamount to refusing to work
  - May be grounds for termination
- Organizations can incorporate confirmation statements into employment contracts, annual evaluations, or other documents necessary for continued employment

Policy Enforcement

- Policy enforcement must be able to withstand external scrutiny
- If an employee is punished, or dismissed as a result of a refusal to follow policy but can demonstrate that the policies were not uniformly applied or enforced
  - The organization may face punitive or compensatory damages

SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems Part 1

- This special publication reinforces a business-process-centered approach to policy management
  - Targeted at U.S. federal agencies but offers a practical approach to InfoSec planning
- **Policy Administrator** - the policy champion position combined with the manager position
  - A mid-level staff member who is responsible for the creation, revision, distribution, and storage of the policy
  - Solicits input from InfoSec experts and business-focused managers

SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems Part 2

- **Review Schedule** - Any policy document should contain a properly organized schedule of reviews
  - A policy should be reviewed at least annually
  - Policy administrator should solicit input from all affected parties and use this input to modify the document accordingly
- **Review Procedures and Practices** - The policy administrator should implement a mechanism by which individuals can easily make recommendations for revisions
  - May need to be anonymous

SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems Part 3

- **Policy and Revision Date** - publishing a policy without a date can create problems if employees are complying with an out-of-date policy
- The policy document should include:
  - Date of origin
  - Dates of revision, if any
- An expiration date prevents a temporary policy from becoming a permanent mistake

A Final Note on Policy

- Policies are meant to inform employees of what is and is not acceptable behavior in the organization
  - Can help organizations avoid litigation
- Policy development is intended to improve employee productivity and prevent potentially embarrassing situations
- Most employees inherently want to do what is right
  - Knowing what is prohibited, what the penalties are, and how penalties will be enforced is a preventative measure that should free employees to focus on business

Summary Part 1

- A quality InfoSec program begins and ends with policy
- Policy drives the performance of personnel in ways that enhance the InfoSec of an organization’s information assets
- Developing proper guidelines for an InfoSec program is a management problem, not a technical one
- InfoSec policies are the least expensive means of control, but they are often most difficult to implement
- Policy is a statement of the organization’s position that is intended to influence and determine important decisions

Summary Part 2

- A policy may be viewed as a set of rules that dictates acceptable and unacceptable behavior within an organization
- Policies must contain information on what is required and what is prohibited, on the penalties or violating policy, and on the appeals process
- For a policy to be effective, it must be properly written, distributed, read, understood, agreed to, and uniformly applied to those for whom it is intended

Summary Part 3

- Management must define three types of InfoSec policies:
  - Enterprise information security program policy
  - Issue-specific information security policies
  - System-specific information security policies