TEL2813/IS2820
Security Management

Lecture 3
Information Security Policy

Jan 29, 2008

Introduction

- Information security policy:
  - What it is
  - How to write it
  - How to implement it
  - How to maintain it
- Policy
  - Essential foundation of effective information security program

Why Policy?

- A quality information security program
  - begins and ends with policy
  - 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
- Some Guidelines
  - It should contribute to the success of the organization
  - Management must ensure the adequate sharing of responsibility for proper use of information systems
  - Involve end users of information systems

Figure 4-1
The Bulls-eye Model

Importance of Policy

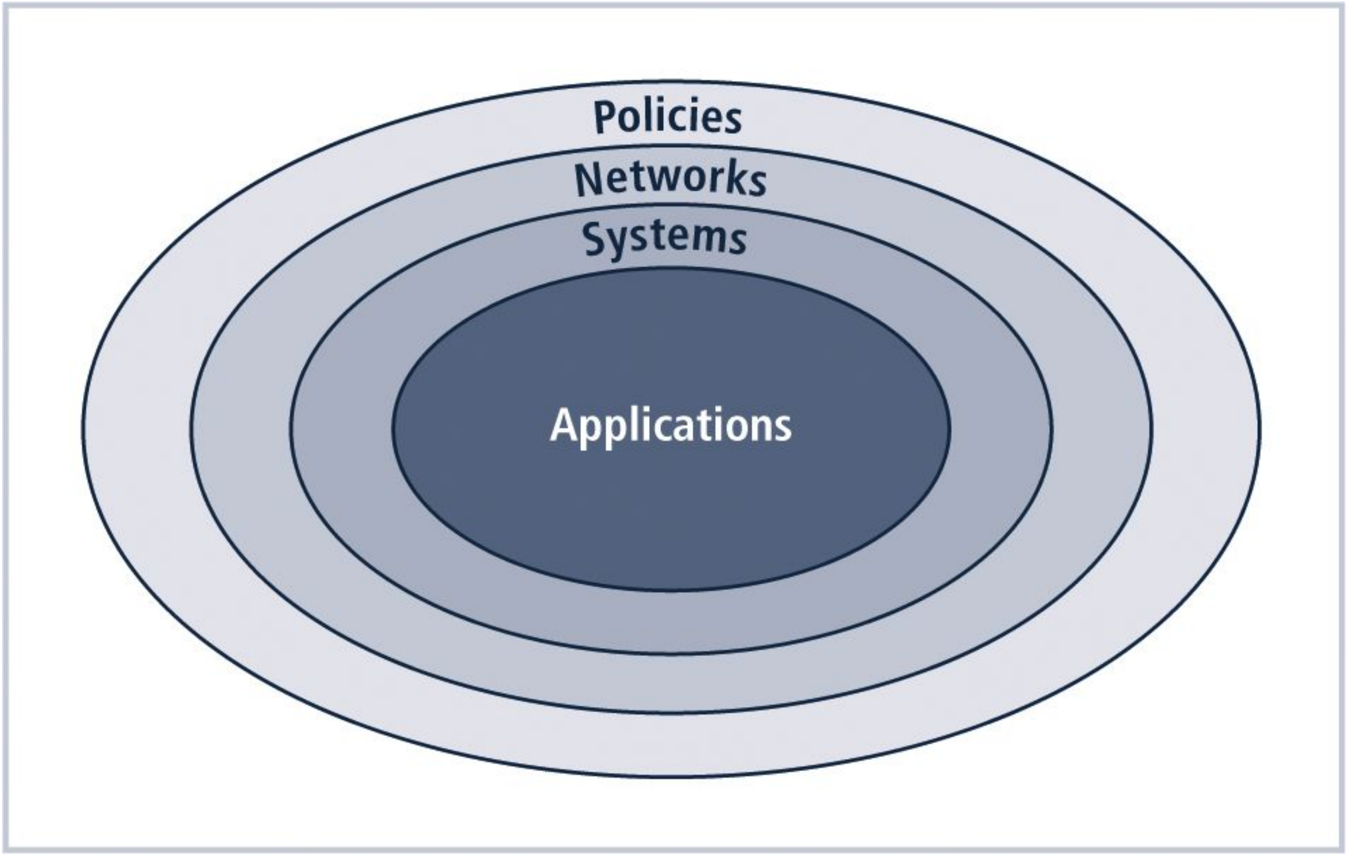


FIGURE 4-1 The Bull's-Eye Model

Policies, Standards, & Practices

Policy: A set of rules that dictates acceptable and unacceptable behavior

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

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

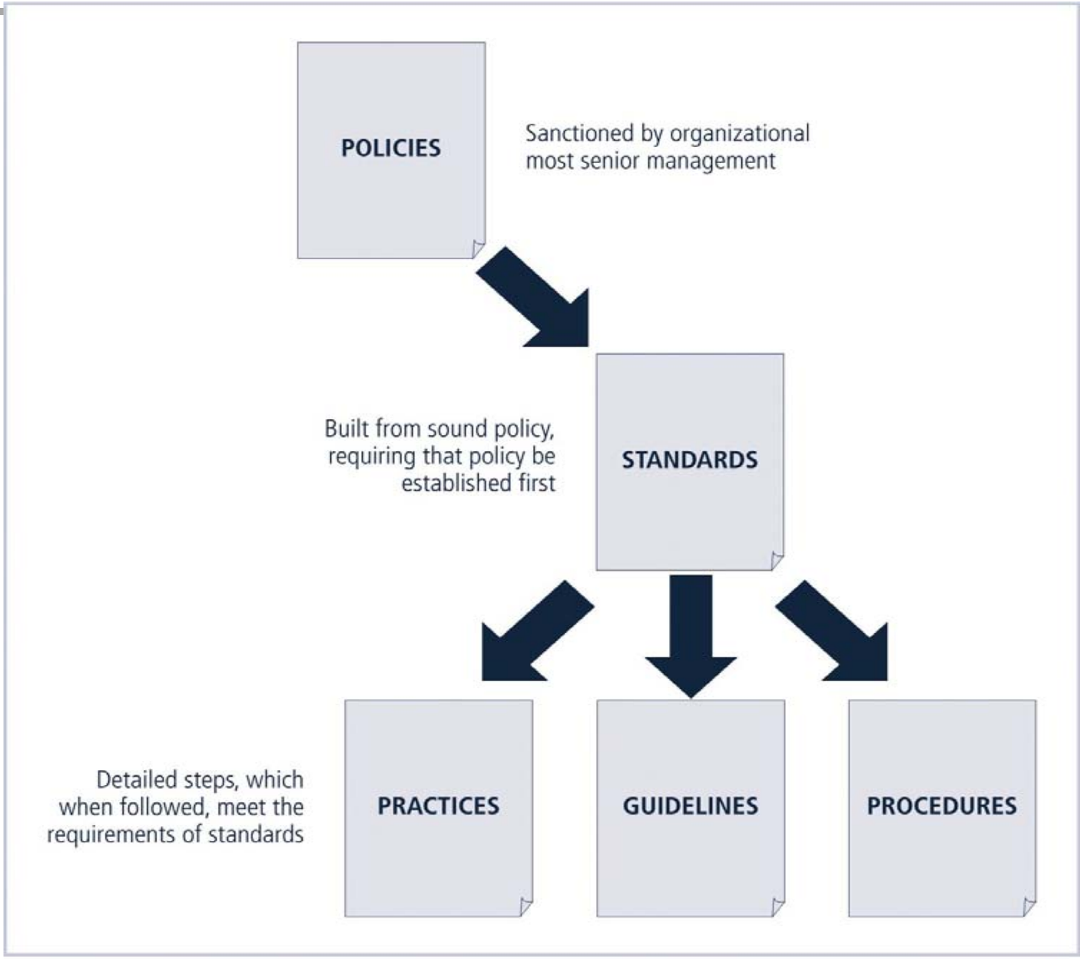

POLICIES
Sanctioned by organizational most senior management
Built from sound policy, requiring that policy be established first
STANDARDS
Detailed steps, which when followed, meet the requirements of standards
PRACTICES
GUIDELINES
PROCEDURES

FIGURE 4-2 Policies, Standards, and Practices

Policy, Standards, and Practices

- For policies to be effective, they must be:
  - Properly disseminated
  - Read
  - Understood
  - Agreed-to
- Policies require constant modification and maintenance

Policy, Standards, and Practices (Continued)

- To produce a complete information security policy, management must define three types of information security policy (NIST 800-14):
  - 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
  - Executive-level document; 2-10 pages
  - CISO in consultation with CIO
- Assigns responsibilities for various areas of information security, including
  - Maintenance of information security policies
  - Practices and responsibilities of end users
- EISP guides
  - The 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 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
- Exceptions To Policies
- Policy Non-Enforcement
- Violation Of Law
- Revocation Of Access Privileges
- Industry-Specific Information Security Standards
- Use Of Information Security Policies And Procedures
- Security Controls Enforceability

Issue-Specific Security Policy (ISSP)

- Every organization’s ISSP has three characteristics:
  - Addresses specific technology-based systems
  - Requires frequent updates
  - Contains an issue statement on the organization’s position on an issue
- ISSP topics could include:
  - E-mail use,
  - Internet and World Wide Web use,
  - Specific minimum configurations of computers to defend against worms and viruses,
  - Prohibitions against hacking or testing organization security controls,
  - ..

Typical ISSP Components

- 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 include creating:
  - a number of independent ISSP documents
  - a single comprehensive ISSP document
  - A modular ISSP document that unifies policy creation and administration
    - Recommended approach
    - It provides a balance between issue orientation and policy management

TABLE 4-4 ISSP 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 over-generalize 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

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
    - Maybe combined in a single policy document

Management Guidance SysSPs

- Created by management
  - guides 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
- ACLs enable administrations to restrict access according to user, computer, time, duration, etc.
- 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

Configuration Rules

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

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

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 Policy Project

- Policy (re)development projects should be
  - well planned,
  - properly funded, and
  - aggressively managed to ensure completion on time and within budget
- Policy development project can be guided by the SecSDLC process
  - Investigation
  - Analysis
  - Design
  - Implementation
  - Maintenance

Investigation Phase

- The policy development team should:
  - Obtain support from senior management (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

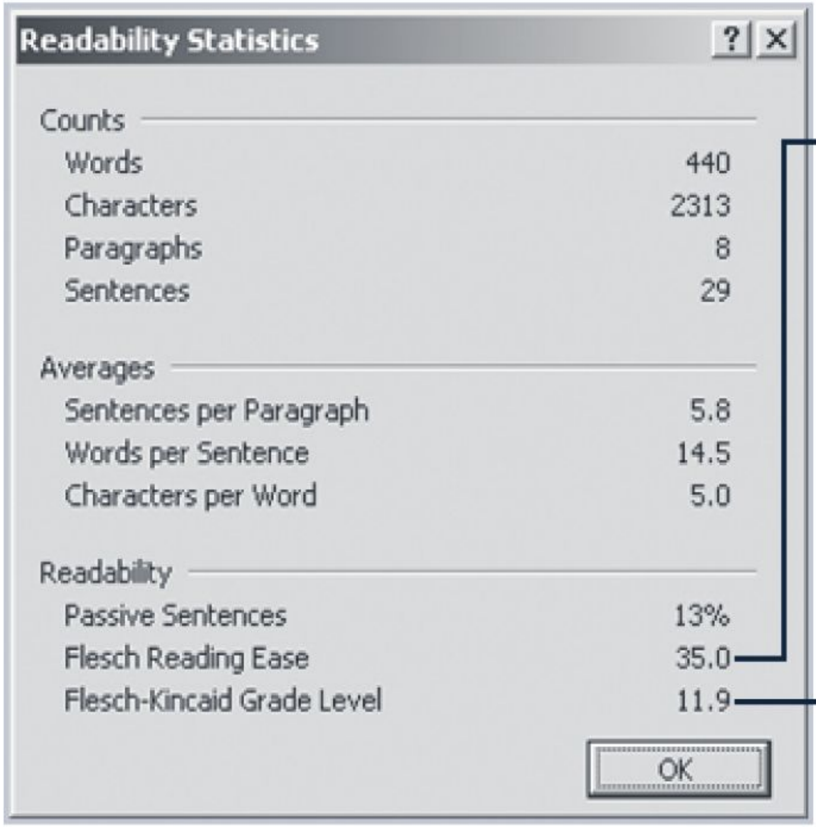
Design Phase

- 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
    - Readability statistics
  - Attempts to minimize technical jargon and management terminology

Readability Statistics Example



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

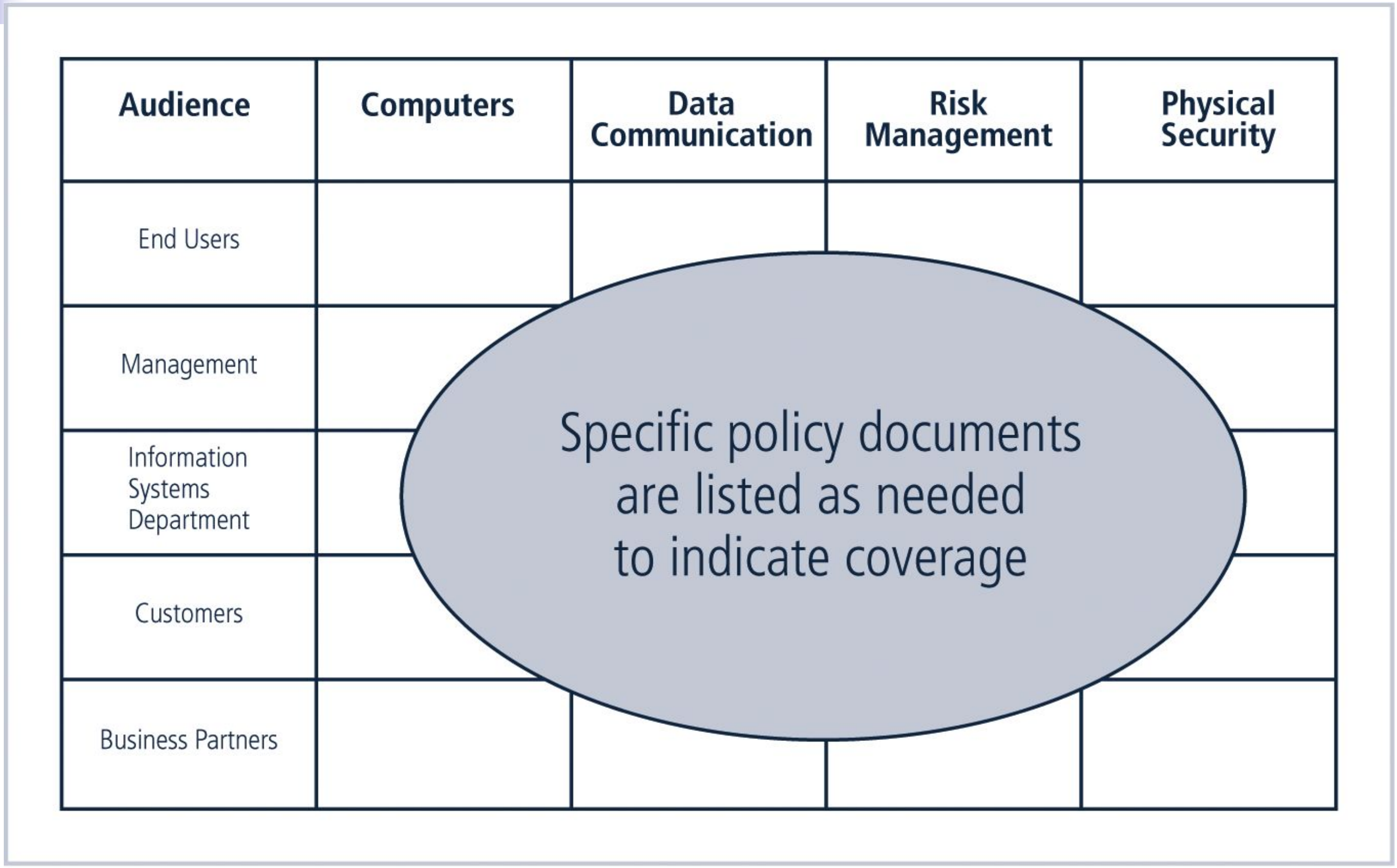
- Maintain and modify policy as needed to ensure that it remains effective as a tool to meet changing threats
- Policy should have a built-in mechanism via which users can report problems with the policy, preferably anonymously
- Periodic review should be built in to the process

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

- Refer to the huge checklist!!

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 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:
  - Documents that constantly change/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

Summary

- 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