Lecture 4: Information Security Policy

EECS 711 Security Management & Audit

Principles of Information Security Management

The focus of the course (six P’s):

1. **Planning**
2. **Policy**
3. **Programs**
4. **Protection**
5. **People**
6. **Project Management**

Chapters 2 & 3

Chapter 4

Introduction

- Information security policy:
  - What it is?
  - Why it is needed?
  - How to write it?
  - How to implement it?
  - How to maintain it?

What is Policy?

- A formal statement of an organization’s managerial philosophy
  - provided by management
  - comprise a set of rules that describe *acceptable and unacceptable behavior* within the organization

- **Information security policies**
  - written instructions to inform employees and others in the workplace of the *proper behavior* regarding use of information and *information assets*

Why need Policy?

“Policies are important reference documents for internal audits and for the resolution of legal disputes about management’s due diligence” and “policy documents can act as a clear statement of management’s intent”

- Charles Cresson Wood

- Explain the will of the organization
- Provide *structure* in the workplace
- Create a productive and effective work environment

Why need Policy?

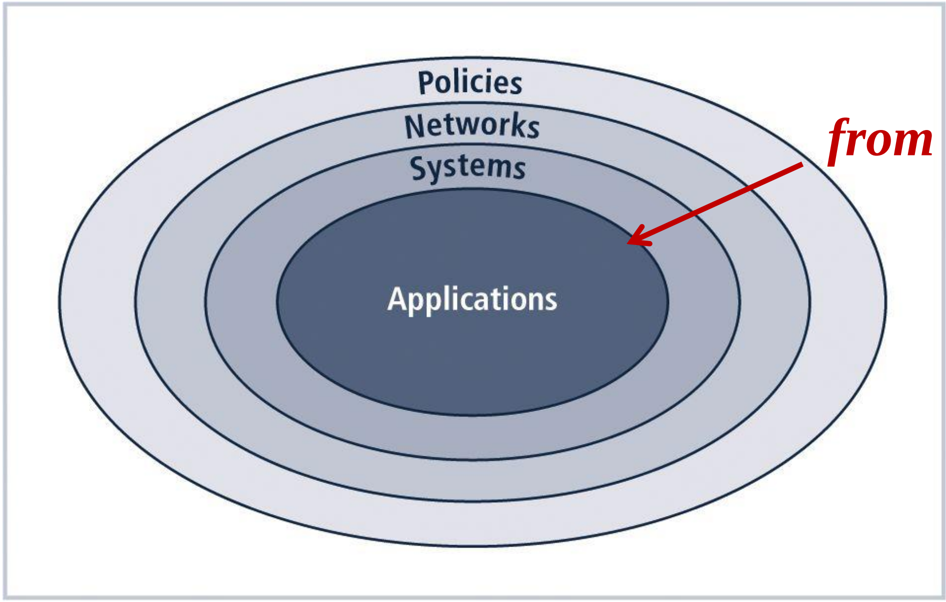
- Policy controls are the least expensive means of control
  - Cost
    - time and effort spent creating, approving, and communicating them
    - time and effort spent integrating them into daily activities
- But the most difficult to implement
  - for policies to be effective, they must be properly disseminated, read, understood, and agreed-to
  - consistently applied
    - e.g., Enron/Anderson scandal

InfoSec Policies

- Policy is the essential foundation of an effective information security program
  - a quality information security program begins and ends with policy
  - 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

The Bulls-eye Model

- An implementation model that emphasizes the role of policy in an InfoSec program
  - provides a mechanism for prioritizing complex changes



from general to specific

FIGURE 4-1 The Bull's-Eye Model

The Bulls-eye Model

- Policy-centric decision making
  - Policies
    - the *initial viewpoint* most users have for interacting with InfoSec
  - Networks
    - *environment* where threats from public networks meet the networking infrastructure
  - Systems
    - *hardware* and *software* as well as *systems* used for process control and manufacturing
  - Applications
    - application systems

How to Develop

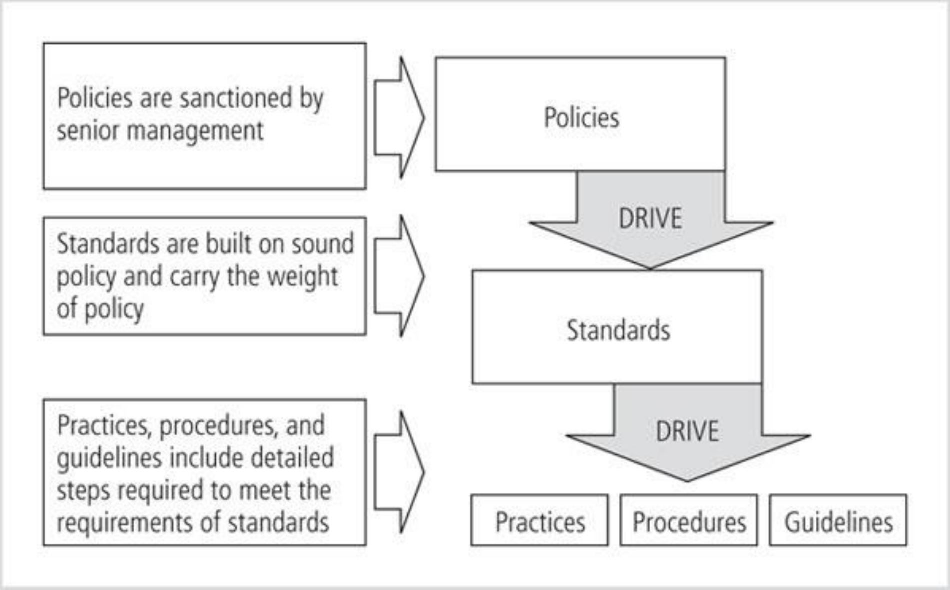
- **Basic rules:**
  - never conflict with law
  - stand up in court if challenged
  - properly supported and administered
- **Guidelines:**
  - must contribute to the success of the organization
    - tailored to the needs: too relaxed or too stringent?
  - management must ensure adequate sharing of responsibility for proper use of information systems
  - involve end users in the steps of policy formulation

Policy, Standards, and Practices

- **Policy**: a plan or course of action intended o influence and determine decisions, actions, and other matters

- **Standard**: a more 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

Policy, Standards, and Practices

- **NIST SP 800-14:** Management must define three types of InfoSec policies:
  - Enterprise information security policy (**EISP**)
  - Issue-specific security policies (**ISSP**)
  - System-specific security policies (**SysSP**)

Enterprise Information Security Policy (EISP)

- **Enterprise information security policy (EISP)**
  - a.k.a. security program policy, general security policy, IT security policy, or InfoSec policy, …
  - highest-level policy
    - drafted by CISO in consultation with CIO
    - 2-10 page *executive-level document*

Enterprise Information Security Policy (EISP)

- Enterprise information security policy (EISP)
  - sets strategic direction, scope, and tone for an organization’s security efforts
    - e.g., an organization responsible for maintaining large mission-critical databases
      - reduction in errors, data loss, data corruption, and recovery
  - assigns responsibilities for various areas of InfoSec
  - assign compliance issues
    - meeting the requirements to establish a program and the responsibilities assigned to organizational components
    - the use of specified penalties and disciplinary actions

Integrating an Organization's Mission and Objectives into EISP

- EISP must support organization's *vision* and *mission* statements
  - an organization's strategic planning
    - → key business unit strategic policies & IT strategic policy
    - → InfoSec strategic planning
  - should not contradict the organizational mission statement
- EISP should state the importance of InfoSec to the organization's mission and objectives
  - guides development, implementation, and management requirements of InfoSec program

EISP Elements

- EISP documents should include:
    - an overview of the corporate philosophy on security
    - information on the structure of InfoSec organization 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

EISP Components

- **Statement of Purpose**
  - what is the policy for?
- **Information Technology Security Elements**
  - defines information security topics and critical components
- **Need for Information Technology Security**
  - justifies the need and importance of InfoSec in the organization
  - including obligations (legal and ethical)
- **Information Security Responsibilities and Roles**
  - defines staffing structure
- **Reference** to other policies, standards and guidelines

Problem-based Learning

- Read KU’s Information Technology Security Policy
  - http://www.policy.ku.edu/IT/info-technology-security-policy
- Identify the key elements in this policy:
  - Overview
  - Structure
  - Responsibilities (shared & individual)
- Identify the key components in this policy:
  - Purpose
  - Elements
  - Need
  - Roles & Responsibilities
  - References

Issue-Specific Security Policy (ISSP)

- **ISSP** provides detailed, targeted guidance to instruct all members of the organization in the *use of a resource*
  - a binding agreement between organization and members
- An effective ISSP can
  - articulate how technology-based systems should be *used*
  - document how technology-based system is *controlled* and identifies the processes and authorities that provide this control
  - indemnify the organization against *liability* for an employee’s inappropriate or illegal use of the system

Typical ISSP Areas

- Use of e-mails, instant messaging (IM), …
- Use of the Internet on company and personal time
- Malware protection requirements
- Use of non-organizationally 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
- Use of personal equipment on company networks
- Use of telecommunications technologies (fax, phone, mobile phone)
- Use of photocopying and scanning equipment

ISSP Components

- **Statement of purpose** - begins 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
  - fair and responsible use
- **Prohibited uses** - outlines what the issue or technology cannot be used for
  - unless a particular use is clearly prohibited, the organization cannot penalize employees for it

ISSP Components (cont.)

- **Systems management** - focuses on the users' relationships to systems management
  - users' and sys admins' responsibilities
- **Violations of policy** - specifies the penalties and repercussions of violating the usage and systems management policies
  - procedures for reporting violations

ISSP Components (cont.)

- **Policy review and modification** - outlines a specific methodology for ISSP review and modification
  - procedures for periodic reviews and modifications
- **Limitation of liability** - offers a general statement of liability or a set of disclaimers

Implementing the ISSP

- Three of the most **common approaches**
  - a number of independent ISSP documents
    - each tailored to a specific issue
  - a single comprehensive ISSP document
    - covers all issues
  - a modular ISSP document
    - unifies policy creation and administration while maintaining each specific issue’s requirements

Implementing the ISSP

- Modular ISSP document
  - a recommended approach
  - use a standard template
    - individual modules: common standardized aspects + customized issues
    - created and updated by responsive individuals
    - reported to a central policy administration group
    - easy to manage and use

Problem-based Learning

- Search the KU policy library to find ISSP policies
  - http://policy.ku.edu/office/Information-Technology
- Answer the questions:
  - How many ISSP KU has? What are they?
  - Which implementation approach does KU IT take to develop the ISSP policies?
    - What’s your clue?

System-Specific Security Policy (SysSP)

- **SysSP** often look differently from the other two policies
  - it functions as standards or procedures to be used when configuring or maintaining systems
  - e.g: to configure/operate a network firewall
- It can be separated into
  - managerial guidance
  - technical specifications
  - or combined in a single unified document

Managerial Guidance SysSPs

- Created by management
  - to guide the implementation and configuration of technology
  - to address the behavior of employees in ways that support the security of information
- Applies to *any technology* that affects the confidentiality, integrity, or availability of information
- SysSPs can be developed at the same time as ISSPs, or in advance of the related ISSPs

Technical Specification SysSPs

- A systems administrator need to *create a technical specification policy to implement a managerial policy*
- Each type of equipment has its own type of policies
- For example:
  - ISSP requires user passwords be changed quarterly
  - SysSP requires a systems administrator to implement a technical control within a specific application to enforce this ISSP policy
  - Think about technical control methods
    - Access control lists
    - Configuration rules

Access Control Lists

- **Access control lists (ACLs)**
  - Include *user access lists*, *matrices*, and *capability tables* that govern rights and privileges
  - Control access to file storage systems, object brokers, or other network communications devices
    - *Who* can use the system
      - Restrict access according to users
    - *What* authorized users can access
      - Restrict access according to computer or even a particular file
    - *When* authorized users can access the system
      - Restrict access according to time or duration
    - *Where* authorized users can access the system from
    - *How* authorized users can access the system
      - Assign privileges as read, write, execute and delete

Configuration Rules

- **Configuration rules**
  - instructional codes that guide the execution of the system when information is passing through it
  - many security systems require specific configuration scripts
    - e.g.: firewalls, intrusion detection and prevention systems, proxy servers
- Rule-based policies are more specific to the operation of a system than ACLs are
  - May or may not deal with users directly

Combination SysSPs

- Many organizations create a single document that combines both elements of
  - Management guidance SysSP
  - Technical specifications SysSP
- While combined SysSP can be confusing, it is also very practical
  - Guidance from both perspectives in a single document
  - Should carefully articulate the required actions for each procedure described

Guidelines for Effective Policy

- Policy is *enforceable* if it is properly designed, developed, and implemented using a process that assures repeatable results
- **Six stages**:
  - 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

The InfoSec Policy Project

- Policy development is viewed as a two-part project
  1. Design and develop policy (or, redesign and rewrite if policy is outdated)
  2. Establish management processes 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
- Use a systems development life cycle (SDCL)
  - Investigation, analysis, design, implementation, and maintenance

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 and a sound **estimate** for cost and scheduling of the project

Analysis Phase

- The analysis phase should include:
  - New or recent risk assessment or IT audit documenting the current InfoSec needs
    - any loss history, past lawsuits, grievances, or other records of negative outcomes from InfoSec areas
  - Key reference materials
    - any existing policies
      - may be housed in human resources, accounting, finance, legal, or corporate security departments

Design Phase

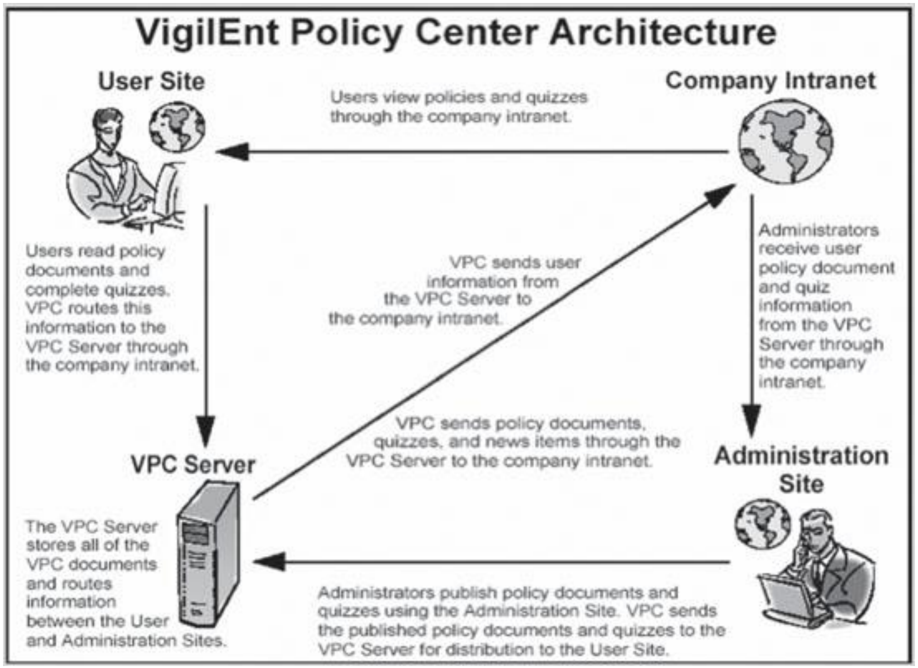
- Design phase should include:
  - How policies will be distributed
  - How verification of distribution will be confirmed
- **Policy distribution**
  - unless the organization can prove that the policy actually reached the end users, it cannot be enforced
  - hard copy distribution
    - insufficient, no guarantee of receiving
  - electronic distribution: email, newsletter, intranet, document management systems
    - easy to send and track
    - best method is electronic policy distribution software

Design Phase

- **Policy verification**
  - Members must explicitly acknowledge that they have received and read the policy
    - Employee’s signature and date provide a paper trail of his or her receipt of the policy
    - Use banners or pop-up windows to display end-user license agreements (EULAs)

Design Phase

- **Use of automated tool**
  - VigilEnt Policy Center – a centralized policy approval and implementation system from NetIQ
    - Allows policy developers to create policy, manage the approval process, and distribute approved policy
    - Assesses readers' understanding of the policy and electronically records reader acknowledgments



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.

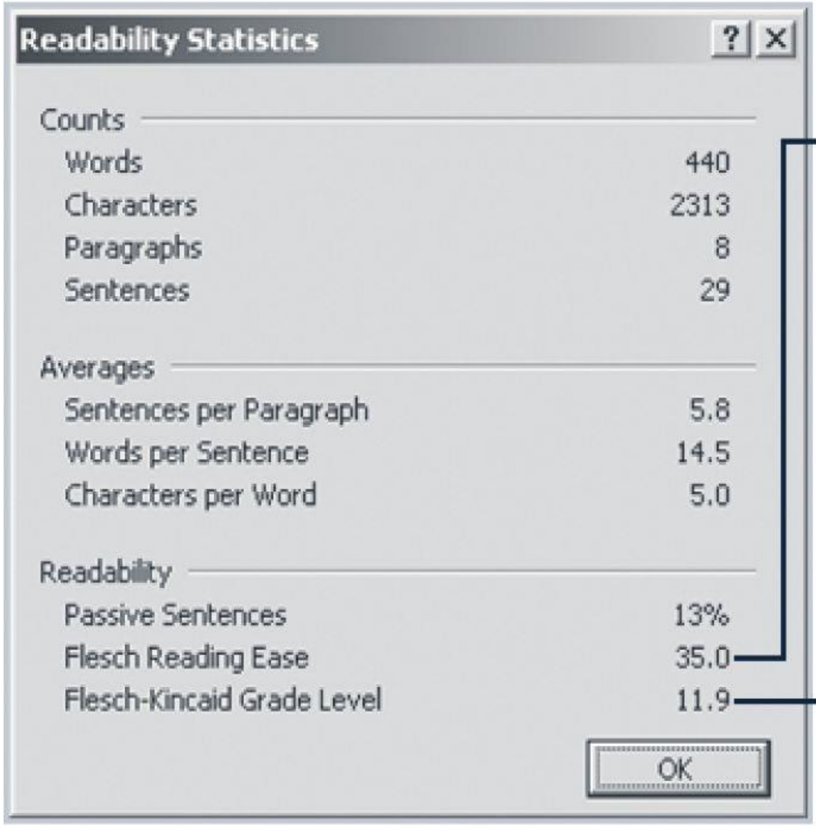
The VPC Server stores all of the VPC documents and routes information between the User and Administration Sites.

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.

Implementation Phase

- Implementation phase: writing the policies
  - Use available resources
    - Web, government sites, professional literature, peer networks, and professional consultants
    - http://www.sans.org/security-resources/policies/
- **Policy reading:**
  - effective policy is written at a reasonable reading level
    - literacy or language barriers
    - additional assistance for the disabled
- **Policy comprehension**
  - readability statistics
  - quizzes and other examinations

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

Implementation Phase

- **Policy compliance**
  - Employee must agrees to the policy
    - failure to agree to a policy equals to refusing to work
  - 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
  - Organization may face punitive or compensatory damages
    - If an employee is punished, censured, or dismissed as a result of a refusal to follow policy
    - But can demonstrate that the policies were not uniformly applied or enforced

Maintenance Phase

- 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 periodical review
  - a built-in mechanism through which users can report problems
    - preferably anonymously

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