CSIT988
Security, Ethics and Professionalism
Lecture 05

Subject Coordinator: *Dr Khoa Nguyen*

School of Computing and Information Technology

Autumn 2025

Roadmap

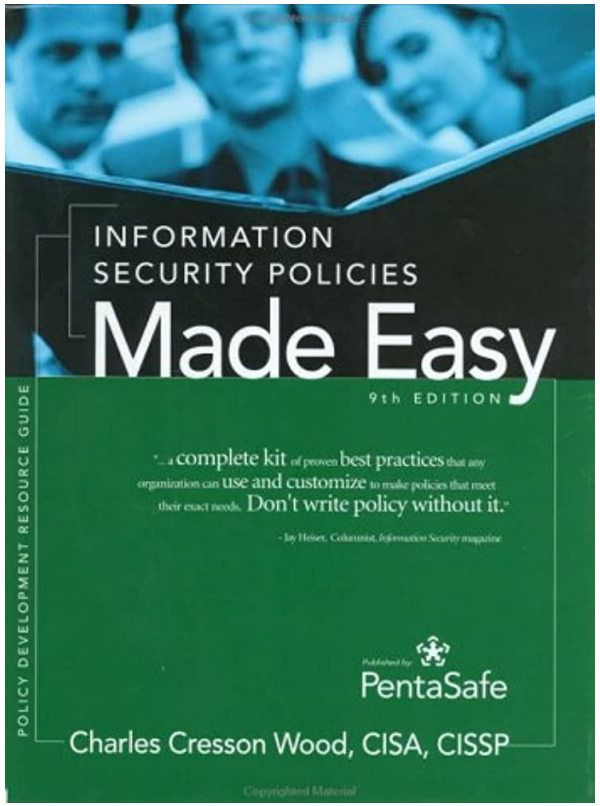
- **Planning for Contingencies**
  - Fundamentals of Contingency Planning
  - Business Impact Analysis
  - Incident Response Plan
  - Disaster Recovery Plan
  - Business Continuity Plan
  - Testing for Contingency Plans

- **Information Security Policy**
  - Why Policy?
  - Enterprise Information Security Policy
  - Issue-Specific Security Policy
  - System Specific Security Policy
  - Guidelines for Effective Policy

Learning Objectives

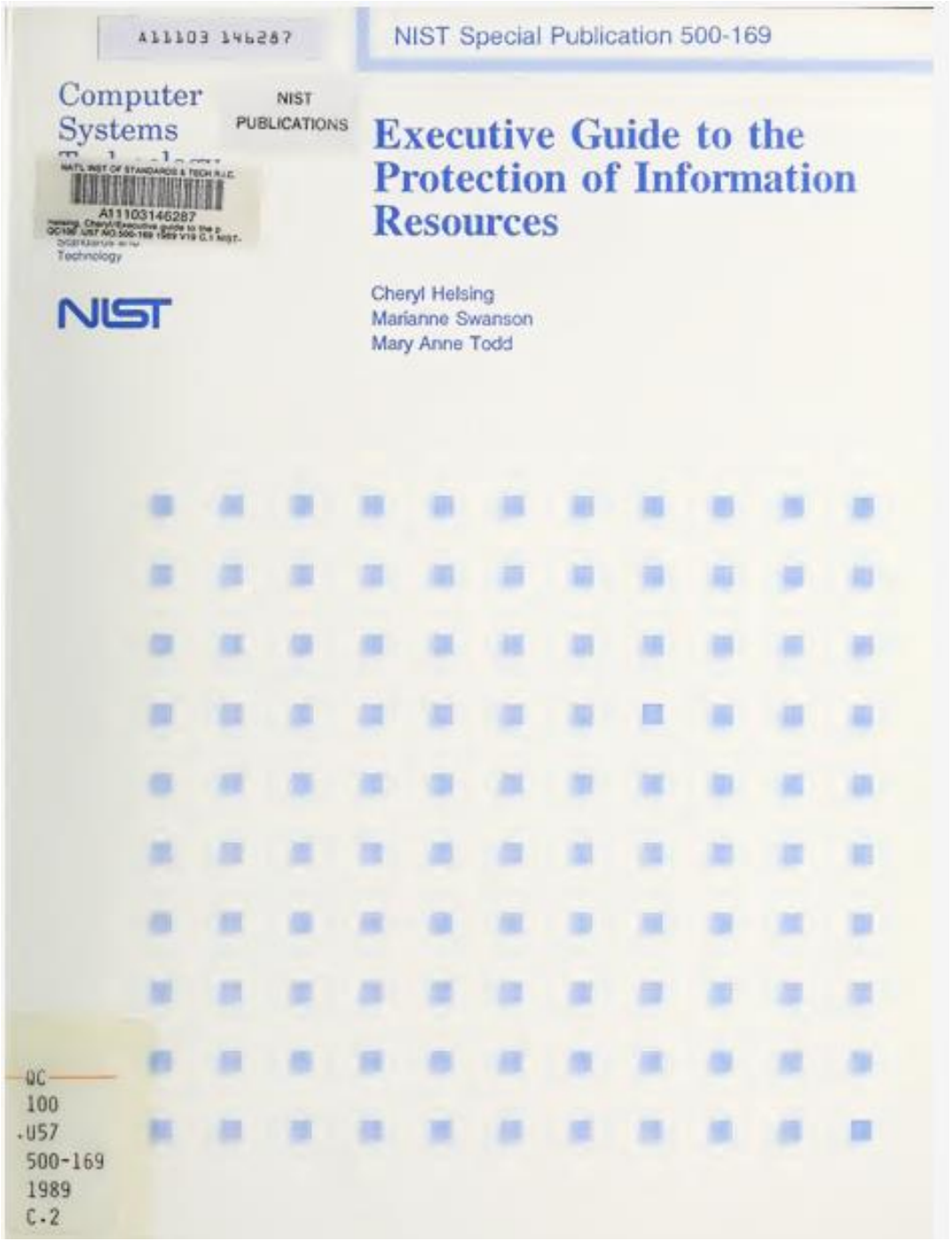
- Define information security policy and understand its central role in a successful information security program
- Describe the three major types of information security policy and discuss the major components of each
- Discuss the process of developing, implementing, and maintaining various types of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

- **In business:** A statement of managerial intent designed to guide and regulate employee behavior in the organization
- **In IT:** A computer configuration specification used to standardize system and user behavior
- **In InfoSec:** Information security policies are written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets



Policy is the essential foundation of an effective InfoSec program.

"The centrality of information security policies to virtually everything that happens in the information security field is increasingly evident. For example, system administrators cannot securely install a firewall unless they have received a set of clear information security policies. These policies will stipulate the type of transmission services that should be permitted, how to authenticate the identities of users, and how to log security-relevant events. An effective information security training and awareness effort cannot be initiated without writing information security policies because policies provide the essential content that can be utilized in training and awareness material."



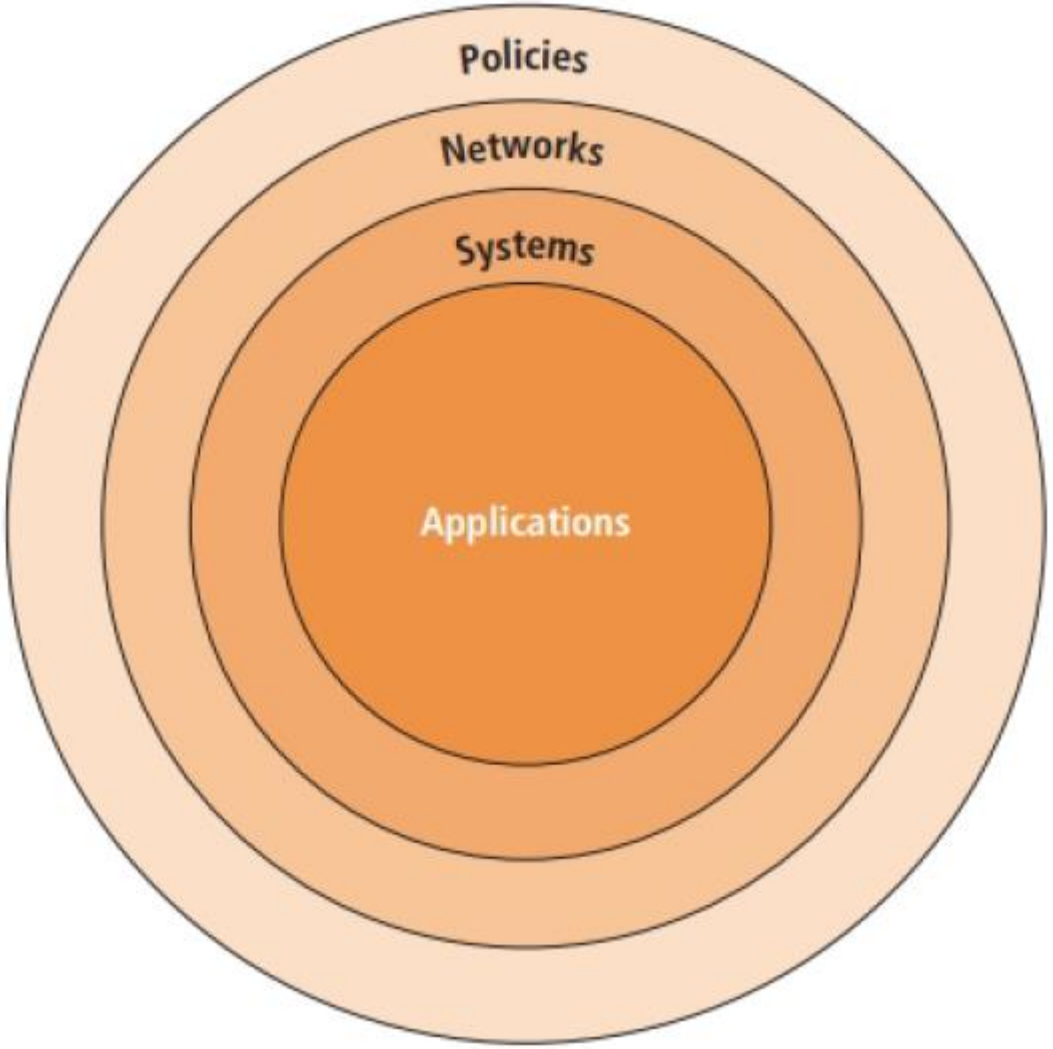
The success of any InfoSec program lies in policy development.

NIST addressed this point in "Special Publication (SP) 500-169, Executive Guide to the Protection of Information Resources":

"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."

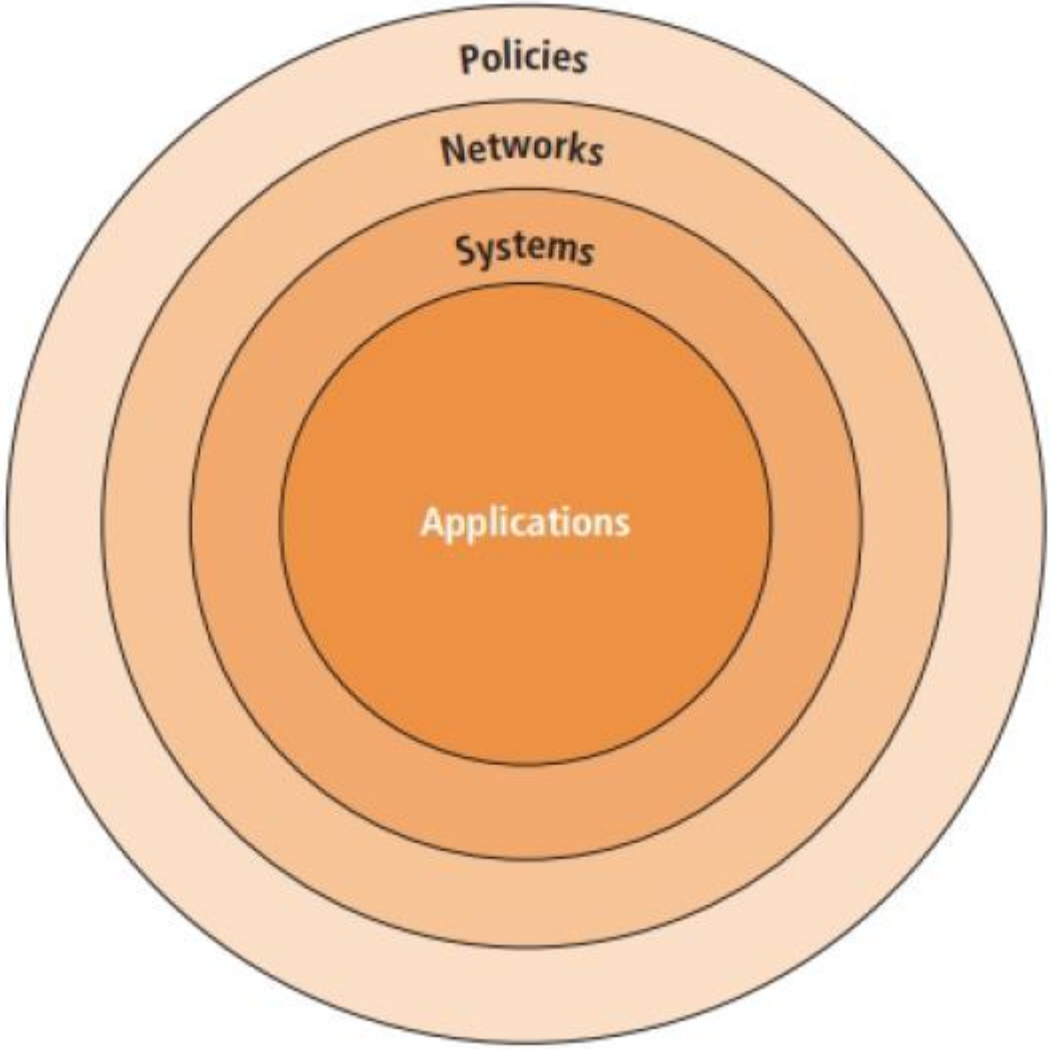
- A quality information security program begins and ends with policy
- InfoSec policies are designed to provide structure in the workplace and explain the will of the management in controlling the behavior of employees regarding the appropriate and secure use of information and information resources.
- Policies are the least expensive means of control and often the most difficult to implement
- Policy must be tailored to the specific needs of the organization.

Bull's-Eye Model



- One implementation model that emphasizes the role of policy in an InfoSec program is the **bull's-eye model**.
- The bull's-eye model has become widely accepted among InfoSec professionals.
- Issues are addressed by moving from the general to the specific, always starting with policy. That is, the focus is on systemic solutions instead of individual problems.
- **Four layers:** Policies, Networks, Systems, Applications

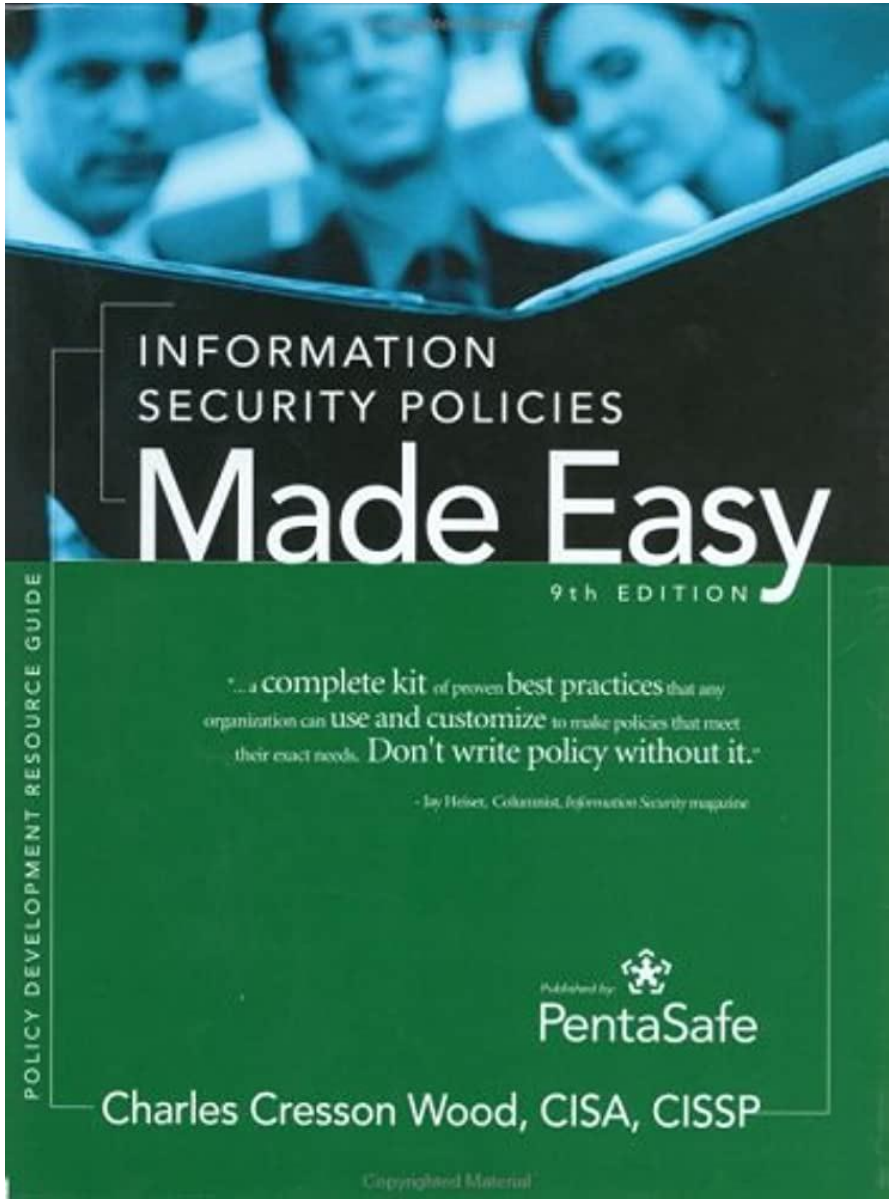
Bull's-Eye Model

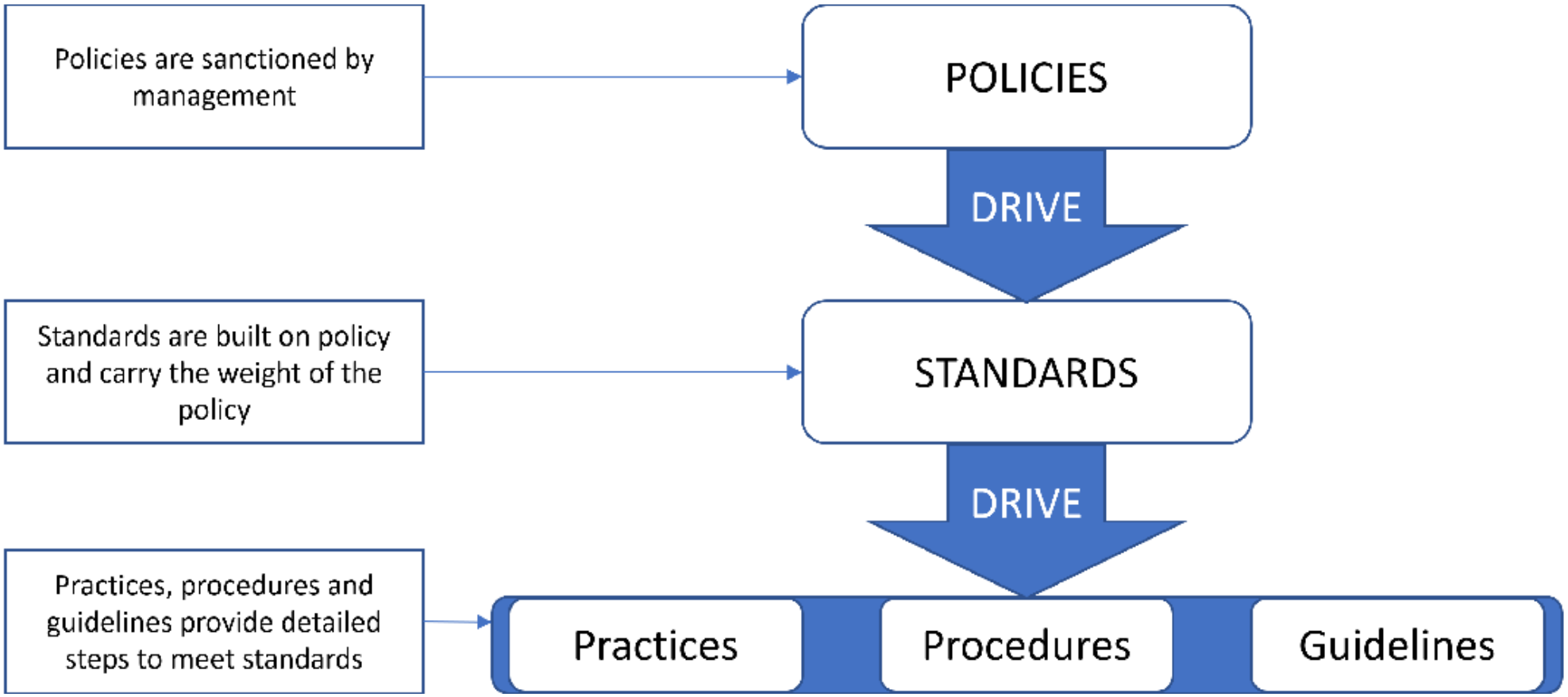


- **Policies:** outer layer; initial viewpoint for most InfoSec system users; available from published documents
- **Networks:** the environment where threats first meet the organization's network
- **Systems:** collections of hardware and software, process control and manufacturing systems
- **Applications:** all applications systems

- In ***Information Security Policies Made Easy,*** Wood summarizes the need for policy as follows:
  - *Policies are important reference documents for internal audits and for the resolution of legal disputes about management's due diligence*
  - *Policy documents can act as a clear statement of management's intent*

- However, policy isn't just a management tool to meet legal requirements. It's necessary to protect the organization and the jobs of its employees.





- **Policy:** A formal statement of the organization's managerial philosophy
- **Standard:** A more detailed statement of what must be done to comply with policy
- **Practices, procedures and guidelines** explain how employees will comply with policy

Types of InfoSec Policies

According to NIST's "Special Publication 800-14", management must define three types of InfoSec policies.

- **Enterprise information security policy (EISP)**
- **Issue-specific security policies (ISSPs)**
- **System-specific policies (SysSPs)**

Each type is found in most organizations.

Enterprise Information Security Policy (EISP)

- **EISP:** High-level InfoSec policy that sets strategic direction, scope, and tone for organization's security efforts
  - a.k.a. "security program policy," "general security policy," "IT security policy," "high-level InfoSec policy," or simply "InfoSec policy"
- Assigns responsibilities for various areas of information security
- Guides development, implementation, and management requirements of information security program
- EISP must directly support the organization's vision and mission statements.

EISP documents should provide:

- An overview of the corporate philosophy on security
- Information on the structure of the 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

- **Purpose:** "What is this policy for?"
- **Elements:** Defines InfoSec, as well as its critical components
- **Need:** Justifies the need to have an InfoSec program in the organization
- **Roles and responsibilities:** Defines the staffing structure for InfoSec
- **References:** Standards that influence and are influenced by this document

Issue-Specific Security Policy (ISSP)

- **ISSP:** An organizational policy providing detailed, targeted guidance to instruct all members of the organization in the use of a resource, e.g., a process or a technology

- ISSP should begin by introducing the organization's resource-use philosophy ➔ protect employees and organization from inefficiency and ambiguity

- An effective ISSP accomplishes the following:
  - Articulate the organization's expectations about how its technology-based system should be used.
  - Document how the 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/illegal use of the system.

ISSP characteristics:

- Address specific technology-based resources
- Require frequent updates
- Contain an issue statement on the organization's position on an issue

Cybersecurity is easy when you write "TOP SECRET" on everything.

Typical ISSP topics:

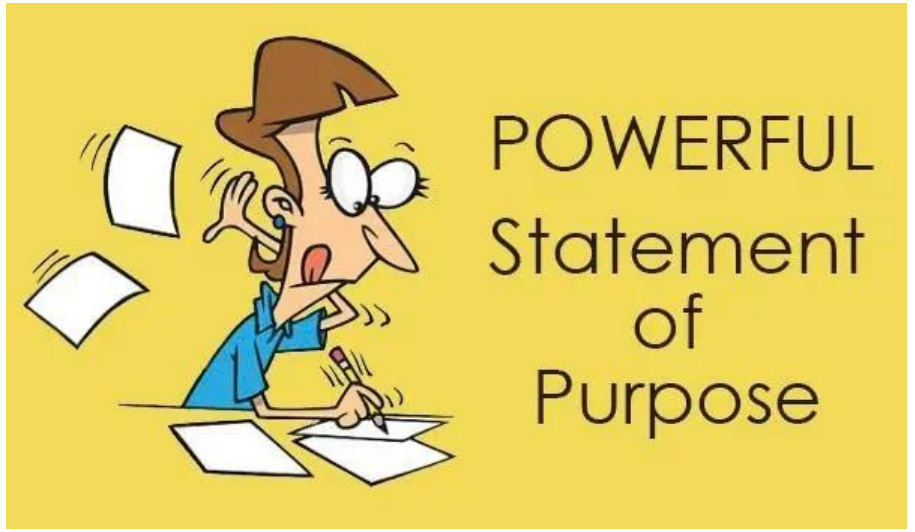
- Email and Internet use
- Malware protection requirements
- Installation and use of non-organizationally issued software or hardware
- Home use of company-owned computer equipment
- Use of personal equipment on company networks
- Use of telecommunications technologies (fax, phone, etc.)
- Use of photocopy/scanning equipment

Components of the ISSP

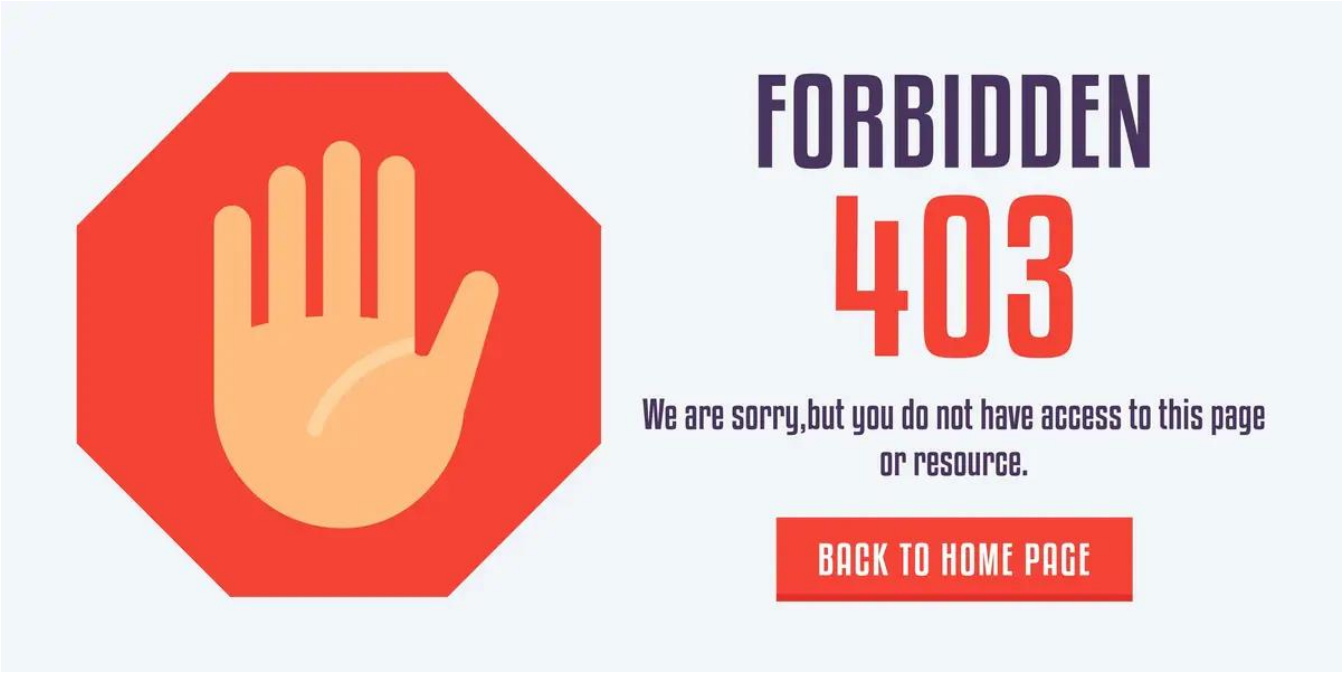
1. Statement of Purpose
2. Authorized uses
3. Prohibited uses
4. System management
5. Violations of policy
6. Policy review and modification
7. Limitations of liability

Components of the ISSP

- **Statement of Purpose**
  - What purpose?
  - Who is responsible?
  - What technologies?



- **Authorized Uses**
  - User access (who can use)
  - Fair and responsible use (legal issues)
  - Specifically defines some selective use of company resources



- **Prohibited Uses**
  - Disruptive use or misuse
  - Criminal use
  - Offensive or harassing materials
  - Copyrighted, licensed or other IP
  - Other restrictions

Components of the ISSP (cont'd.)

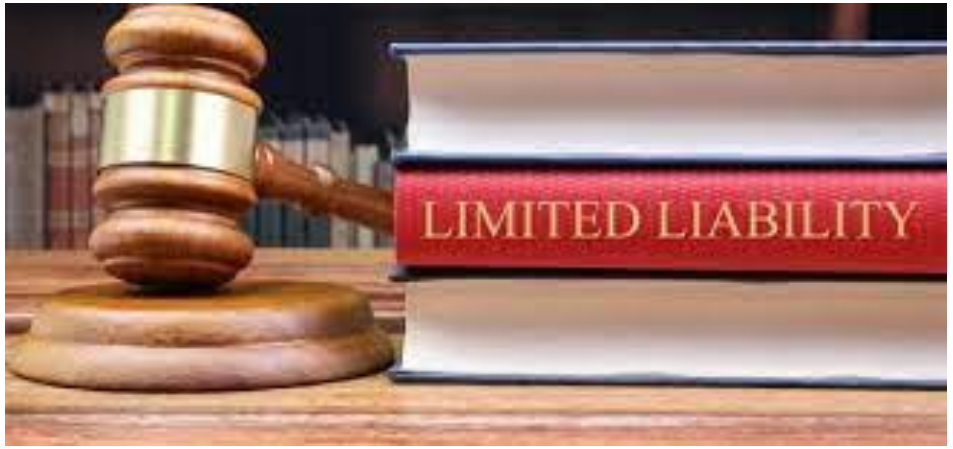
- **Systems management**
  - Focuses on the users' relationships to system management
  - Specifies users' and systems administrators'' responsibilities

- **Violations of policy**
  - Penalties for violations
  - Procedures for reporting violations
  - Anonymous submission are often used

Components of the ISSP (cont'd.)

- **Policy review and modification**
  - Scheduled review of policy and procedures for modification

- **Limitations of liability**
  - Statements of liability or disclaimers
  - The company is not liable for employee's individual actions



Implementing the ISSP

- **Common approaches**
  - Several independent ISSP documents
  - A single comprehensive ISSP document
  - A modular ISSP document that unifies policy creation and administration
- **Recommended approach:** modular policy

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

- **SysSPs** frequently do not look like other types of policy: They may function as standards or procedures to be used when configuring or maintaining systems
  - ➢ e.g., to configure and operate a network firewall.

- SysSPs can be separated into:
  - ➢ Management guidance
  - ➢ Technical specifications

  … or combined in a single policy document

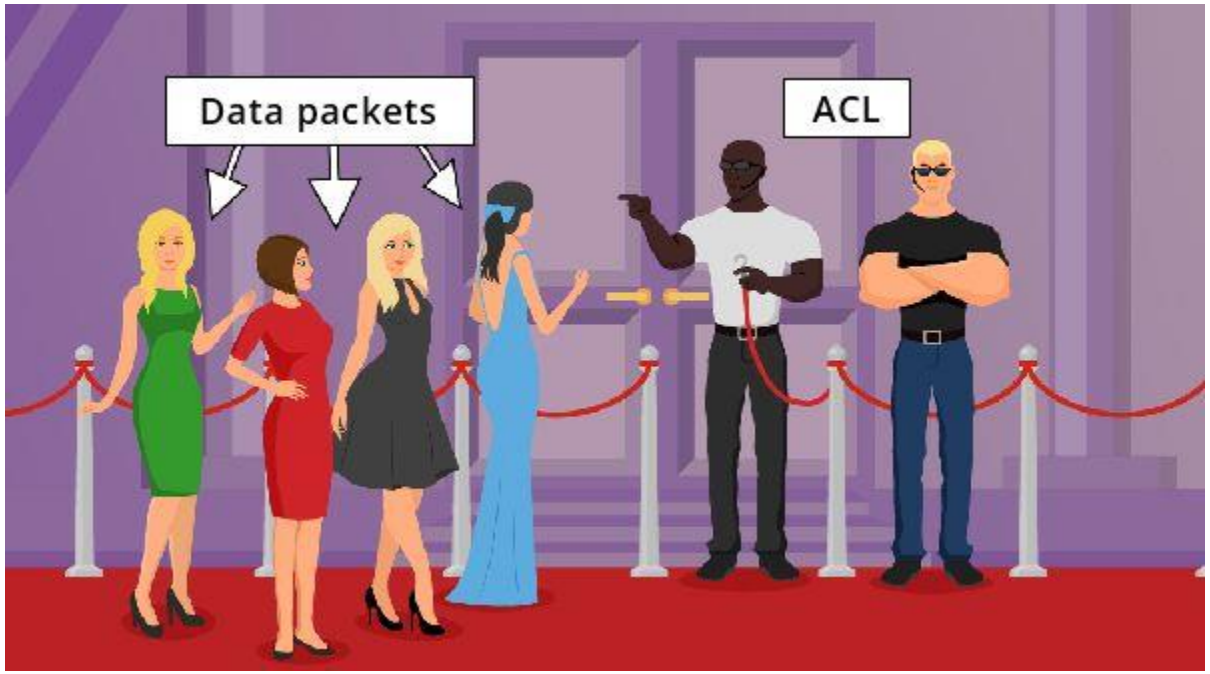
Managerial Guidance SysSPs

- 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
- General methods of implementing technical controls
  - Access control lists
  - Configuration rules

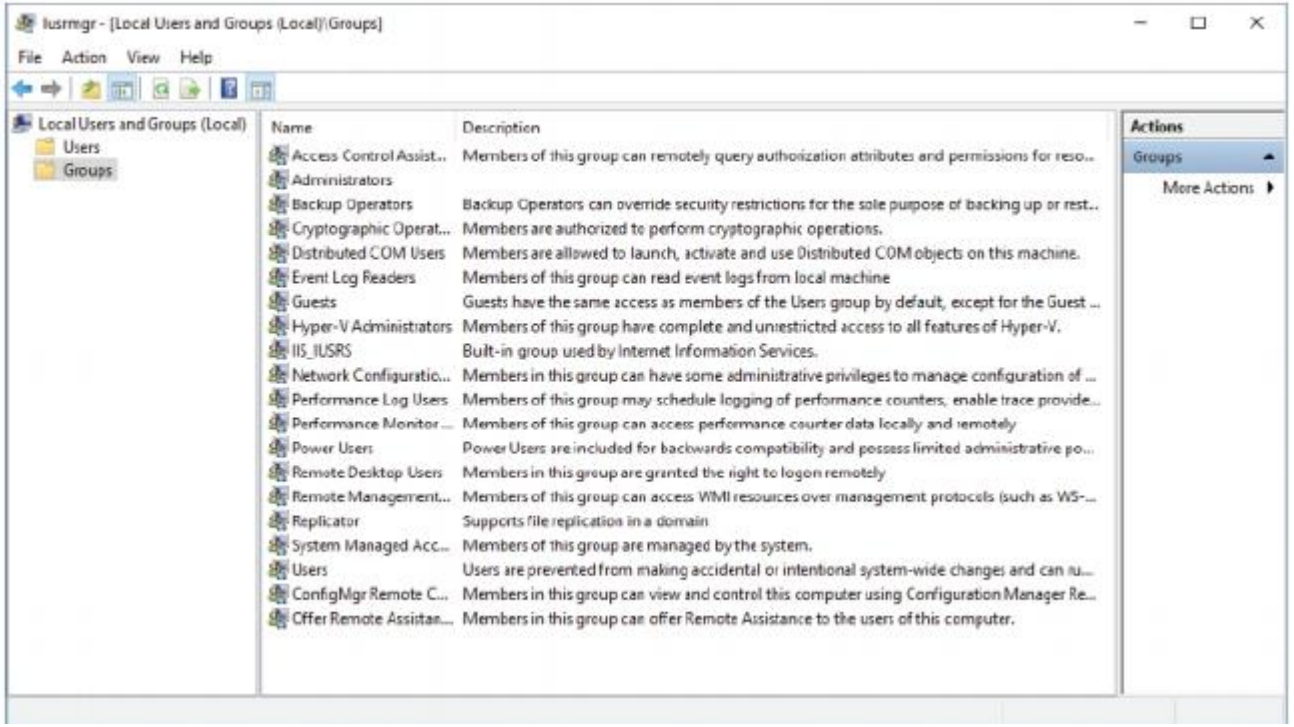
- **Access control lists (ACLs):** Specifications of authorization that govern the rights and privileges of users to a particular information asset
  - ➢ Include the user access lists, matrices, and capability tables that govern the rights and privileges
  - ➢ These specifications are frequently complex matrices, rather than simple lists or tables

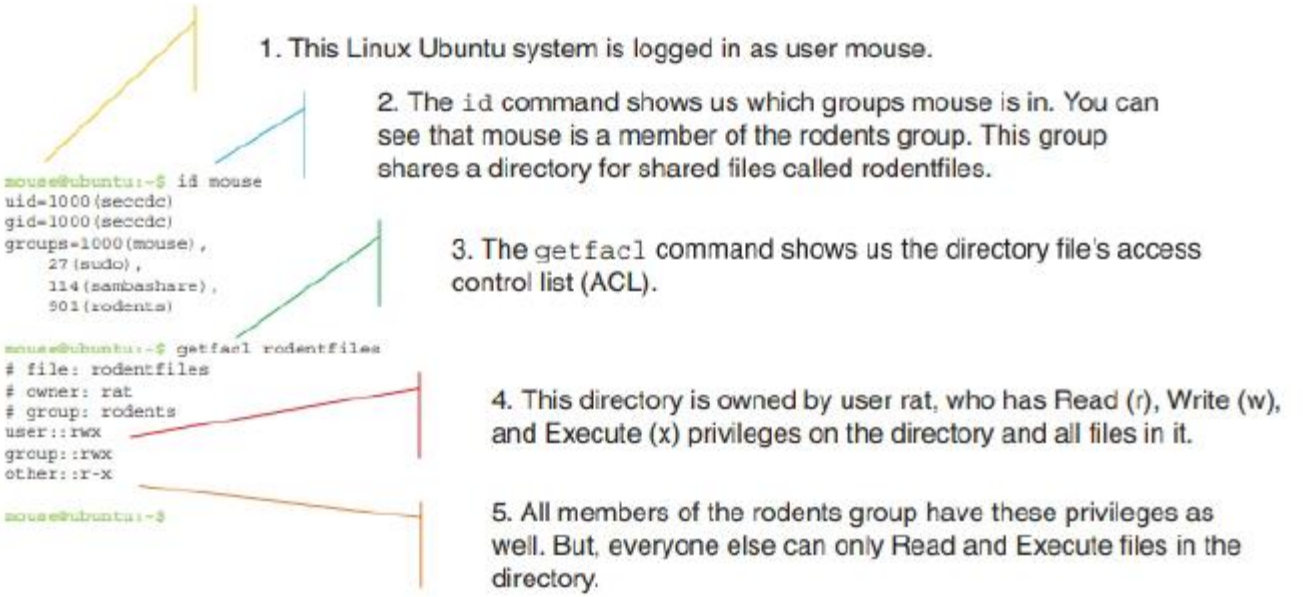


Access control lists regulate

- **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

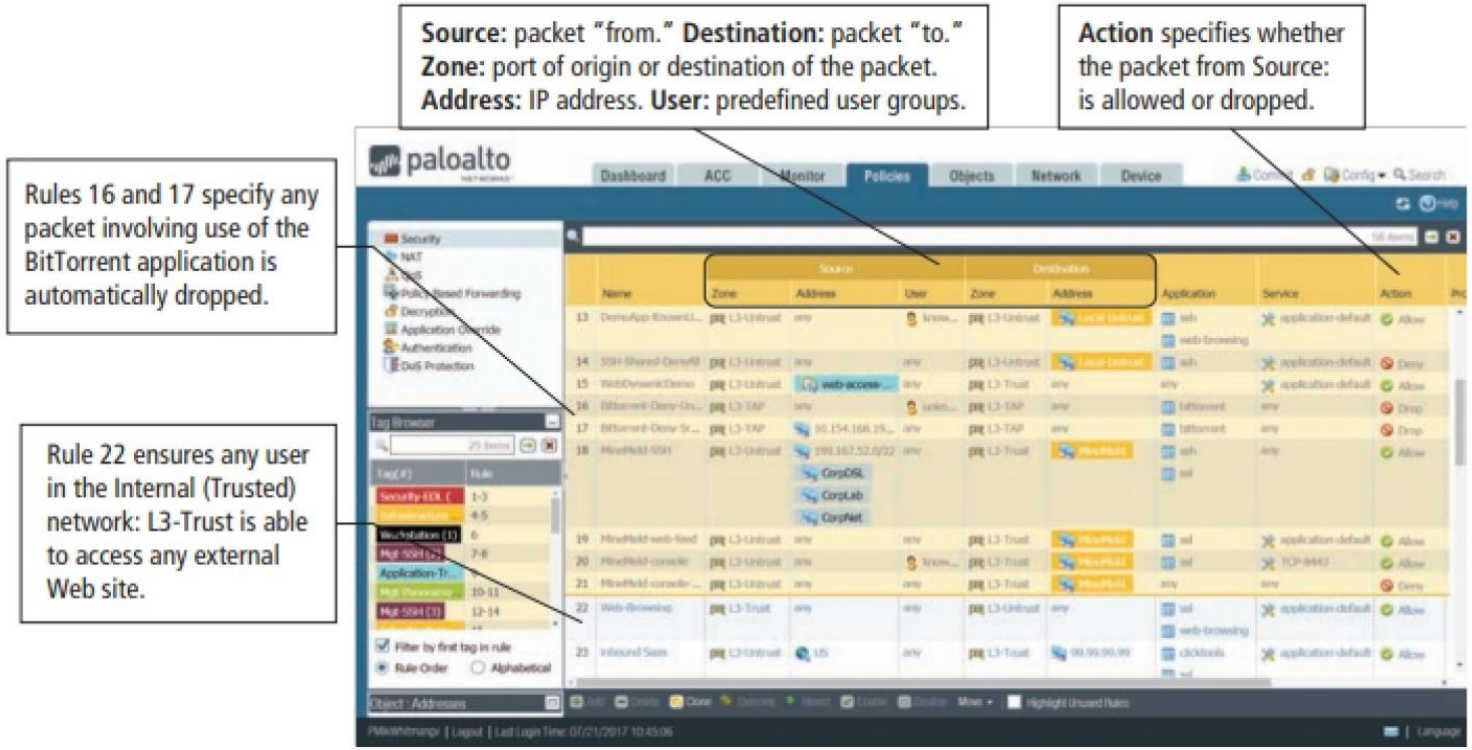
Administrators set user privileges: read, write, create, modify, delete, compare, copy





- **Configuration rules:** instructional codes that guide the execution of the system when information is passing through it

- Rule-based 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 the systems what actions to perform on each set of information they process



Technical Specifications SysSPs (cont'd.)

- Often organizations create a single document combining elements of both management guidance and technical specifications SysSPs
  - ➢ This can be confusing, but practical
  - ➢ Care should be taken to articulate the required actions carefully as the procedures are presented

Guidelines for Effective Policy

- Policy is only enforceable if properly designed, developed, and implemented using a process that assures repeatable results. One effective approach has six stages:
  1. Development
  2. Dissemination (distribution)
  3. Review (reading)
  4. Comprehension (understanding)
  5. Compliance (agreement)
  6. Uniform enforcement

- For policies to be effective, they must be properly:
  1. Developed using industry-accepted practices
  2. Distributed or disseminated using all appropriate methods
  3. Reviewed or read by all employees
  4. Understood by all employees
  5. Formally agreed to by act or assertion
  6. Uniformly applied and enforced

Developing InfoSec Policy

- It is often useful to view policy development as a two-part project
  1. Design and develop the policy (or redesign and rewrite an outdated policy)
  2. Establish management processes to perpetuate the policy within the organization

- A policy development project should be well-planned, properly funded and aggressively managed to ensure completion time and within budget

- The policy development project can be guided by the SecSDLC process
  - **Investigation, analysis, design, implementation, maintenance**

Developing Information Security Policy (cont'd.)

- **Investigation phase**
  - Obtain support from senior management, and active involvement of IT management, specifically the CIO
  - Clearly articulate the goals of the policy project
  - Gain participation of correct individuals affected by the recommended policies
  - Involve legal, human resources and end-users
  - Assign a project champion with sufficient stature and prestige
  - Acquire a capable project manager
  - Develop a detailed outline of and sound estimates for project cost and scheduling

Developing Information Security Policy (cont'd.)

- **Analysis phase** should produce
  - ➢ New or recent risk assessment or IT audit documenting the current information security needs of the organization
  - ➢ Key reference materials
    - ✓Including any existing policies

Developing Information Security Policy (cont'd.)

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

Developing Information Security Policy (cont'd.)

- **Implementation phase** includes
  - Writing the policies
  - Ensuring that the policy is prepared correctly, distributed, read, understood, and agreed to by those to whom it applies, and that those individuals' understanding and acceptance of the policy are documented

Developing Information Security Policy (cont'd.)

- **Maintenance phase**
  - ➢ Maintain and modify the policy as needed to ensure that it remains effective as a tool to meet changing threats
  - ➢ The 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

Policy distribution

- Policy distribution can require a substantial investment by the organization in order to be effective.
- The most common alternatives are hard copy distribution and electronic distribution.

Policy Reading and Comprehension

- **Policy reading**
  - Barriers to reading policies can arise from literacy/language issues.
  - Many jobs do not require literacy skills. Workers must be made familiar with the policy even if it must be read to them.

- **Policy comprehension**
  - Document must be written at a reasonable reading level, with minimal technical jargon and management terminology.
  - Use some form of assessment to gauge how well employees understand the policy's underlying issues.

Policy Compliance and Enforcement

- **Policy compliance:** employees must agree to the policy.
  - ➢ Organizations can incorporate policy confirmation statements into employment contracts, annual evaluations, etc.

- **Policy enforcement**: must be uniform and impartial.

A Final Note on Policy

- Policies exist, first and foremost, to inform employees of what is and is not acceptable behavior in the organization

- Policy development is meant to improve employee productivity, and prevent potentially embarrassing situations

- A quality InfoSec program begins and ends with policy
- Policies must contain information on what is required and prohibited, on the penalties for violating policy, and on the appeals process
- Supporting guidance for policy comes from standards, practices, procedures, and guidelines
- Three types of InfoSec policies: EISP, ISSPs, SysSPs
- Effective policies: properly written, distributed, read, understood, agreed, to, and uniformly applied
- Policy is often developed using a project management approach like SDLC