Chapter 4: Information Security Policy

Gonzalo De La Torre Parra, Ph.D.

Fall 2021

Policy

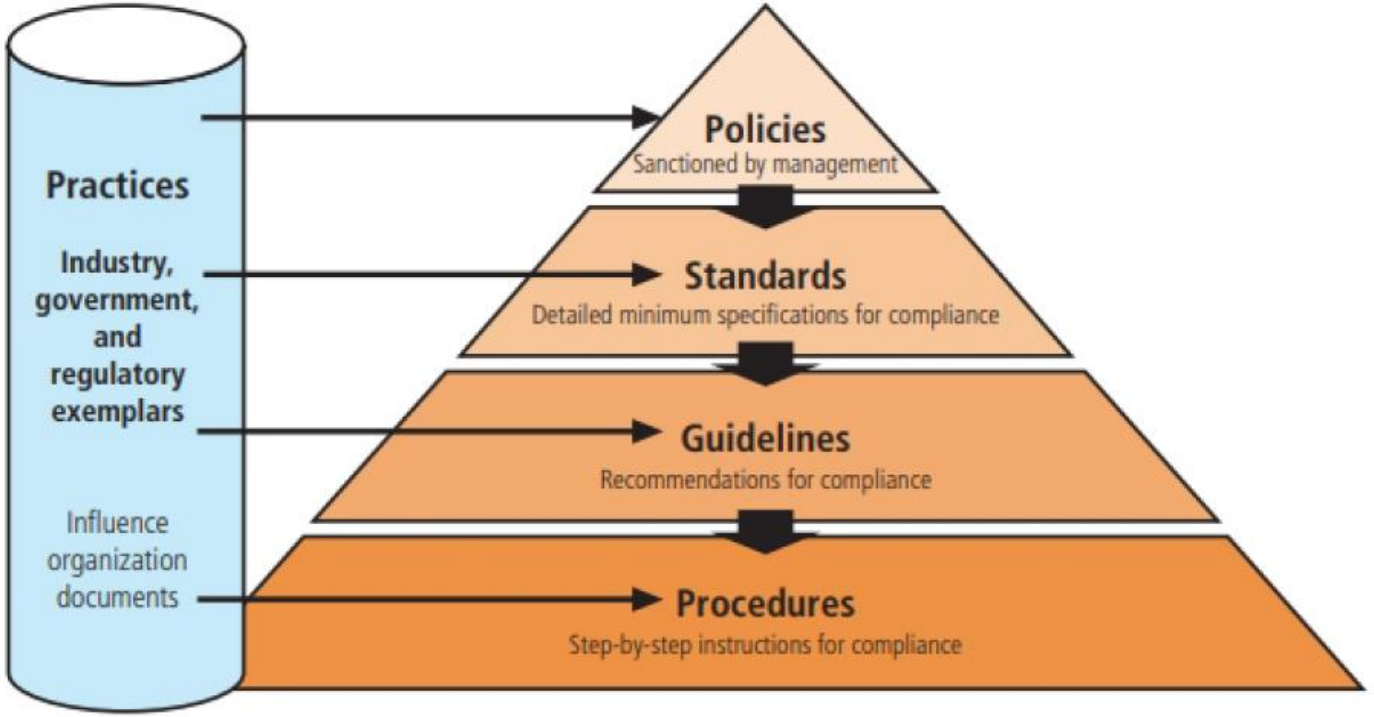
- Policy represents a formal statement of the organization's managerial philosophy in our case, the organization's InfoSec philosophy.
- Policies must also specify the penalties for unacceptable behavior and define an appeals process. For example, an organization that prohibits the viewing of inappropriate
- Web sites at the workplace must implement a set of standards that clarifies and defines exactly what it means by "inappropriate;· and what the organization will do to stop the behavior.

Policies, Standards, and Practices

- **Practices** Examples of actions that illustrate compliance with policies. If the policy states to "use strong passwords, frequently changed," the practices might advise that "according to X, most organizations require employees to change passwords at least semiannually.“
- **Procedures** Step-by-step instructions designed to assist employees in following policies, standards and guidelines. If the policy states to "use strong passwords, frequently changed,“ the procedure might advise that "in order to change your password, first click on the Windows Start button, then .... "
- **Standard** A detailed statement of what must be done to comply with policy, sometimes viewed as the ru les governing policy compliance. If the policy states that employees must "use strong passwords, frequently changed," the standard might specify that the password "must be at least 8 characters, with at least one number, one letter, and one special character."

Relationship

- Practices, procedures, and guidelines explain how employees are to comply with policy.



Enterprise Information Security Policy (EISP)

- Assigns responsibilities for the various areas of InfoSec
- These include maintenance of InfoSec policies and the practices and responsibilities of end users.
- In particular, the EISP guides the development, implementation, and management requirements of the InfoSec program, which must be met by InfoSec management and other specific security functions.

Integrating an Organization's Mission and Objectives into the EISP

- Example: Suppose that an academic institution's mission statement promotes academic freedom, independent research, and the relatively unrestricted pursuit of knowledge.
- What is the tolerance tolerance in the use of organizational technology?
- What is the commitment to protecting the intellectual property of the faculty?
- What is the degree of freedom for study that delves into what could be described as specialized or sensitive areas?

EISP Elements

- 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 (employees, contractors, consultants, partners, and visitors)
- Fully articulated responsibilities for security that are unique to each role within the organization

Sample of EISP Document Elements

1. Protection of Information	
Policy:	Information must be protected in a manner commensurate with its sensitivity, value, and criticality.
Commentary:	This policy applies regardless of the media on which information is stored, the locations where the information is stored, the systems technology used to process the information, or the people who handle the information. This policy encourages examining the ways information flows through an organization. The policy also points to the scope of Information Security management's work throughout, and often even outside, an organization.
Audience:	Technical staff

Sample of EISP Document Elements

2. Use of Information	
Policy:	Company X information must be used only for the business purposes expressly authorized by management.
Commentary:	This policy states that all nonapproved uses of Company X information are prohibited.
Audience:	All

Sample of EISP Document Elements

6. Exceptions to Policies	
Policy:	Exceptions to information security 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, and where this form has been approved by both Information Security management and Internal Audit management.
Commentary:	Management will be called upon to approve certain exceptions to policies. This policy clarifies that exceptions will be granted only after a risk acceptance form has been completed, signed, and approved. The form should include a statement in which the data owner or management takes responsibility for any losses occurring from the out-of-compliance situation. The existence of such a form provides an escape valve that can be used to address situations in which users insist on being out of compliance with policies. All out-of-compliance situations should be made known and documented so that if a loss occurred as a result, management could demonstrate to a judge or jury that it was aware of the situation, examined the risks, and decided to waive the relevant policy or standard.
Audience:	End users

Sample of EISP Document Elements

8. Violation of Law	
Policy:	Company X management must seriously consider prosecution for all known violations of the law.
Commentary:	This policy encourages the prosecution of abusive and criminal acts. While a decision to prosecute will be contingent on the specifics of the case, management should not dismiss prosecution without review. This policy may be important in terms of communicating to those would-be perpetrators of abusive or criminal acts. Many computer crimes are not prosecuted and perpetrators often know this, expecting victim organizations to terminate them and suppress the entire affair.
Audience:	Management

Issue-Specific Security Policy

- An organizational policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resource, such as one of its processes or technologies.
- Also referred to as fair and responsible use policies.

ISSP accomplishes the following:

- It articulates the organization's expectations about how its technology-based resources should be used.
- It documents how the technology-based resource is controlled and identifies the processes and authorities that provide this control.
- It indemnifies the organization against liability for an employee's inappropriate or illegal use of the resource.

ISSP Characteristics

- It addresses specific technology-based resources.
- It requires frequent updates.
- It contains a statement explaining the organization's position on a particular issue.

ISSP is designed to be exemplary, not comprehensive:

- Use of e-mail, instant messaging (IM), and other electronic communications applications
- Use of the Internet, the Web, and company networks by company equipment
- Malware protection requirements (such as anti-malware software implementation)

Elements of the ISSP

- **Statement of Purpose**: outlines the scope and applicability of the policy.
- It should address the following questions:
  - What purpose does this policy serve?
  - Who is responsible and accountable for policy implementation?
  - What technologies and issues does the policy document address?

Elements of the ISSP

- Authorized Uses: Who can use the technology governed by the policy and for what purposes.
- Prohibited Uses: What it cannot be used for. Unless a particular use is clearly prohibited, the organization cannot penalize employees for it.
- Systems Management: Users' relationships to systems management. This section should address management of physical systems as well as electronic systems. The Systems Management section should specify users' and systems administrators' responsibilities, so that all parties know what they are accountable for.

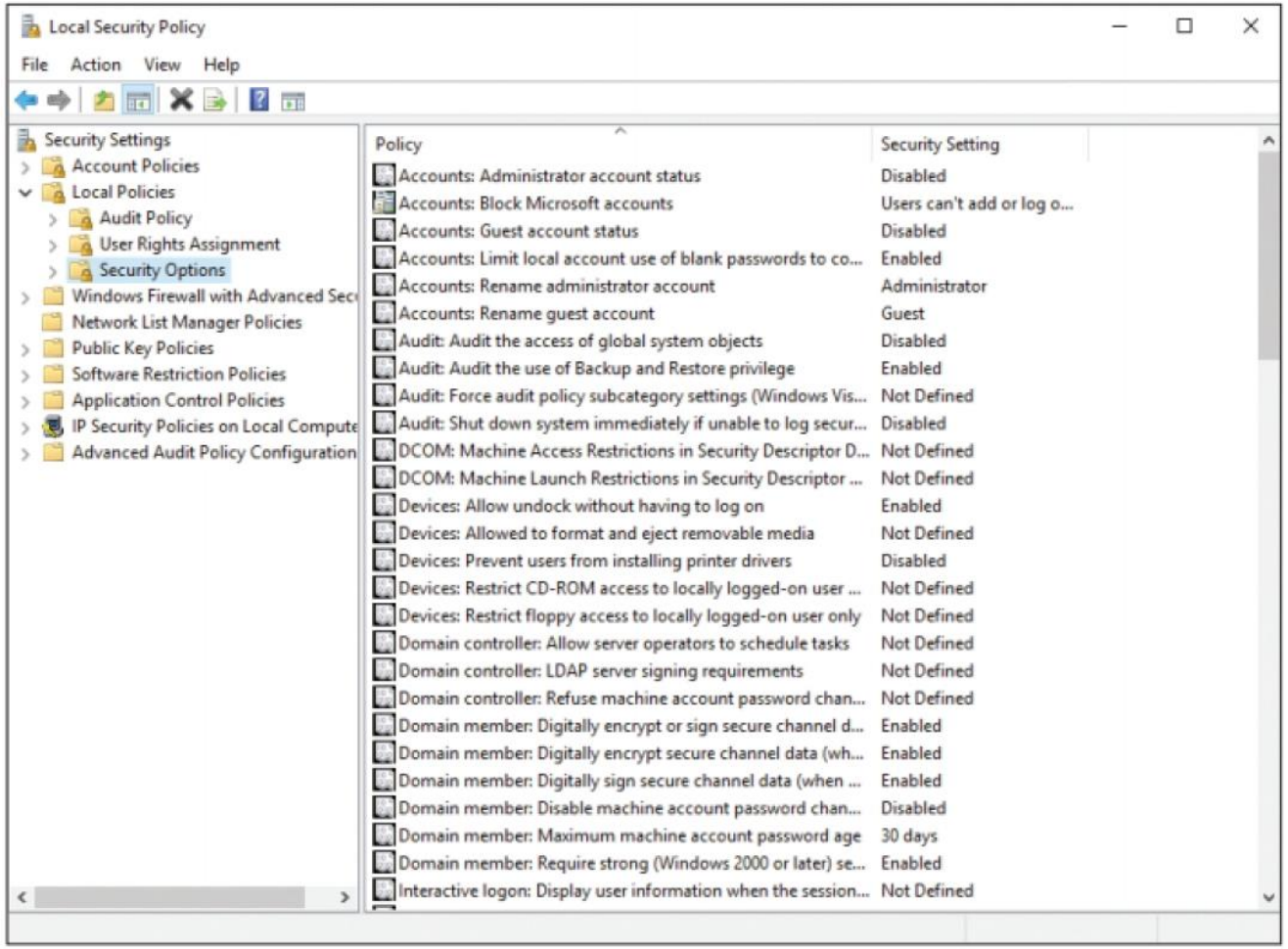
Elements of the ISSP

- Violations of Policy: This section specifies the penalties and repercussions of violating the usage and systems management policies. Penalties should be laid out for each violation.
- Policy Review and Modification: Every policy should contain procedures and a timetable for periodic review.
- Limitations of Liability: general statement of liability or a set of disclaimers. If an individual employee is caught conducting illegal activities with organizational equipment or assets, management does not want the organization to be held liable.

System-Specific Security Policy (SysSPs)

- EISP: high-level policy.
- ISSP: a policy document that may contain procedural elements
- Both are formalized as written documents easily identifiable as policy.
- SysSPs: function as standards or procedures to be used when configuring or maintaining:
  - Configuration and operation of a network firewall.

Windows Local Security Policy



Access Control Lists

- Access control lists (ACLs) include the user access lists, matrices, and capability tables that govern the rights and privileges of users.

- *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

ACLs Cont.

- Restricting who can use the system requires no explanation.

- Read
- Write
- Execute
- Delete

Linux ACLs

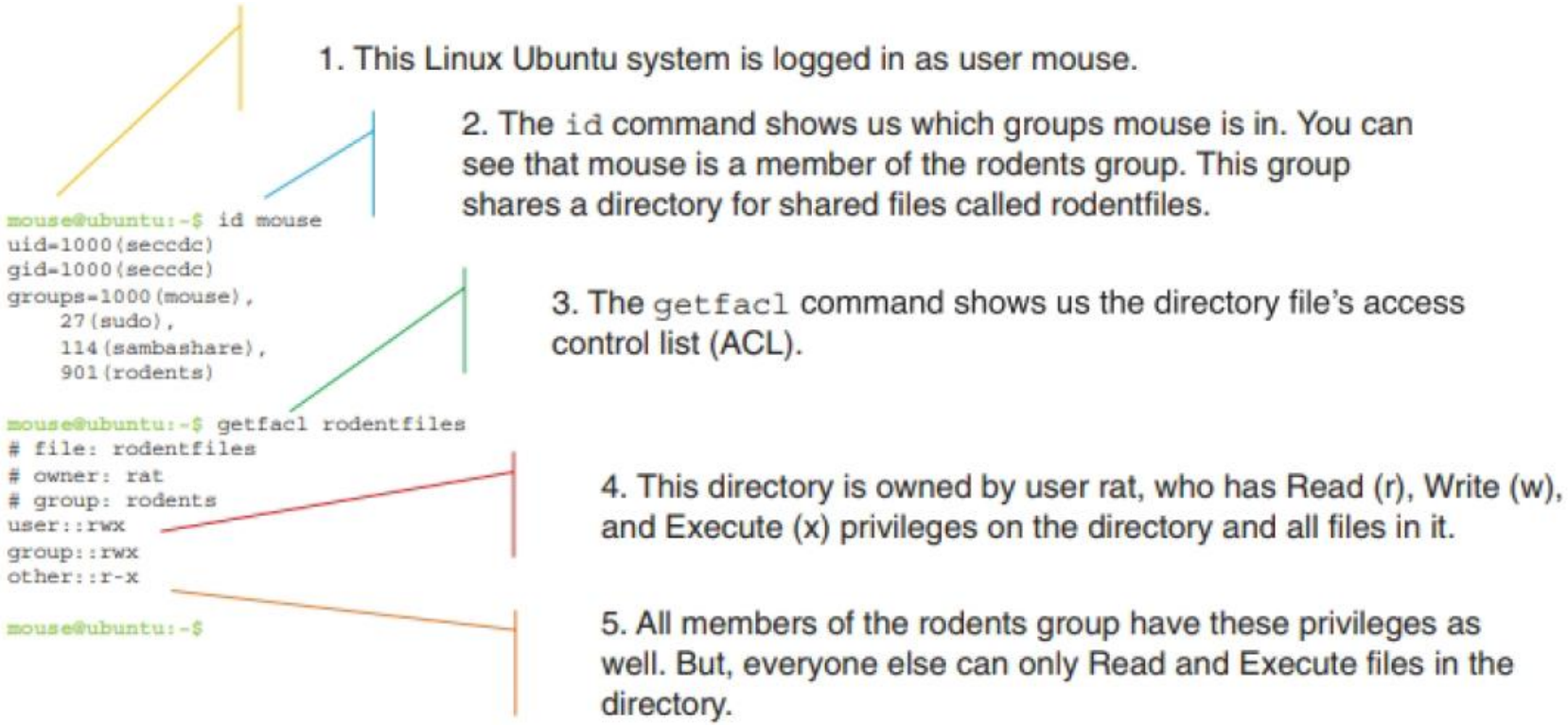


Figure 4-6 Linux ACL

Source: Linux.

Palo Alto Firewall

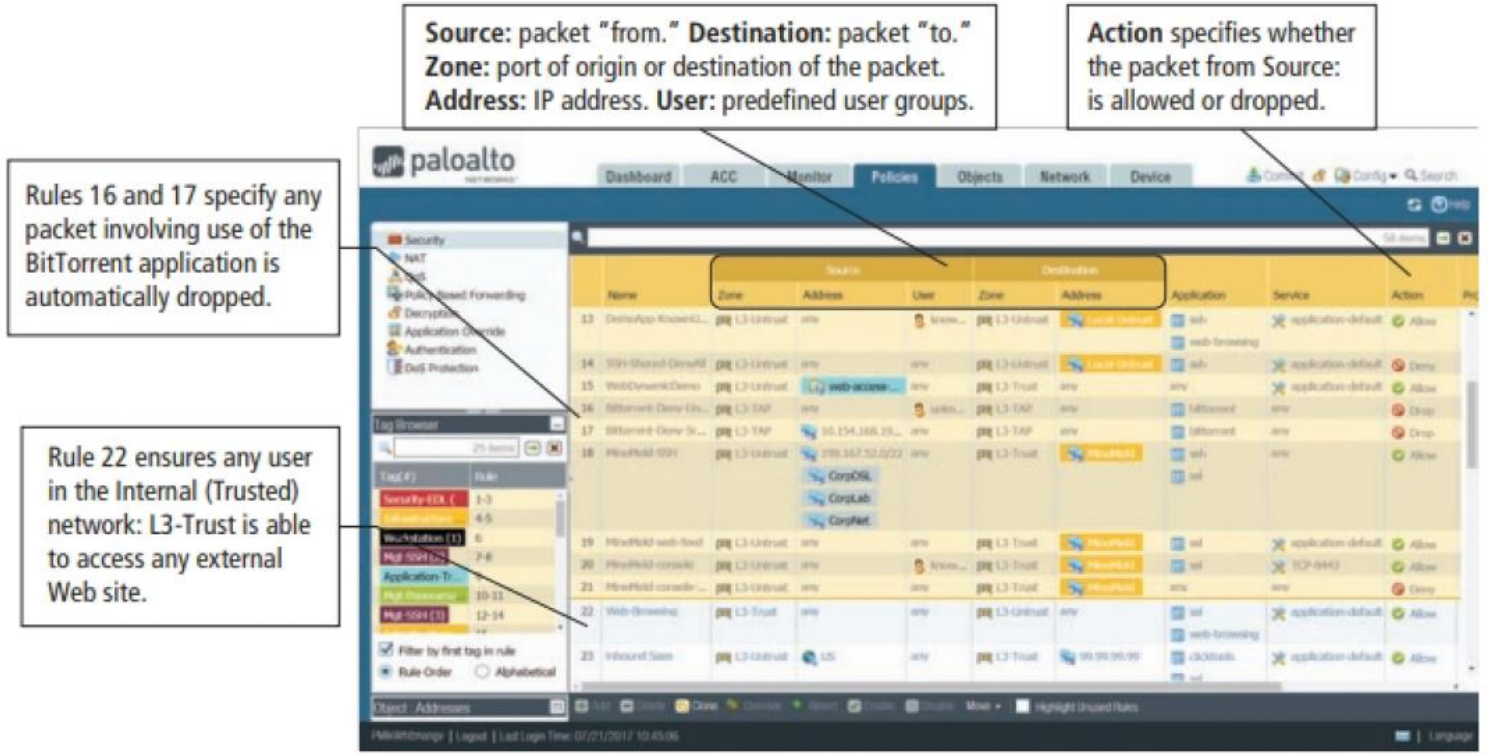


Figure 4-7 Sample Palo Alto firewall configuration rules

Source: Palo Alto Software, Inc.