



# Policy Construction Guidelines

## Differentiating Policies from Other Governance Directives

**Policy**—High-level statement of organizational goals, objectives, and beliefs and a description of the general approach for achieving them with respect to a specified subject area.

**Standards**—Mandatory activities, rules, regulations, or actions that provide specific, non-optional direction in support of a policy.

**Guidelines**—General statements that provide a framework within which to implement procedures. Where standards are mandatory, guidelines are recommendations.

**Procedures**—The step-by-step specifics of how the policy and the supporting standards and guidelines will actually be carried out.

---

## Policy—Standard—Procedure Examples

### EXAMPLE A:

**Policy:** Claims should be processed as quickly as possible

**Standard:** Each claim must be processed within six working days of a receipt.

### Guidelines:

Suspicious claims should be checked against fraud lists and referred to the legal department for further investigation. See Claims Processing/Fraud Guidelines manual for further information.

### Procedure:

Day 1—Set up a file for correspondence, receipts

Day 2—Verify data

Day 3—Adjudicate the claim

Day 4—Enter data into the system

Day 5—Print check

Day 6—Mail check.



### **EXAMPLE B: (Policy—Standard—Guidelines--Procedures)**

**Policy:** Access to company information systems is restricted to authorized users only.

**Standard:** Users are required to have a unique UserID and a confidential password.

**Guidelines:**

Passwords should be a mix of alphanumeric characters

IDs should be traceable to a specific user user. Default or anonymous ids should be avoided.

**Procedure:**

- 1) Prior to creating and distributing a User ID and default password, an approval from management must be obtained. The approval must contain a handwritten signature.
  - 2) Check the signature against the Signature Reference Manual
  - 3) Create and distribute the default ID, requiring returning receipt
  - 4) Verify that default password has been changed within 3 days
  - 5) Contact user if default password has not been changed within 3 days, and walk the user through the process on the phone.
- 

## **Quality Characteristics**

- Be easy to understand
  - Be applicable
  - Be achievable
  - Be enforceable
  - Be proactive
  - Avoid non-conformance absolutes
  - Meet business objectives
- 

## **Policy Types**

**Program**—Used to create the overall vision of an organization.

**Topic-specific**—Addresses specific topics of concern

**Technology specific**—Focus on decision taken by management in connection with specific applications.

---

**Quality Systems are Secure Systems!**

---



## DEPTH & DETAIL

The nature of the topic should govern the policy depth and detail. For instance:

- a) a topic like “Access Control” represents an entire domain area of control. Therefore, policy depth and detail should be high level. (“information assets must be protected”)
- b) a topic like “User Access Management is one of the several areas that fall within the Access Control Domain. Therefore, it should cover the general information about the topic at a moderate detail level. (“user access will be protected using these defined approaches and strategies”)
- c) a topic like “User IDs” is still a topic found in the “Access Control Domain” and under the “User Access Management” policy area, but will be even more specific than the other two (“one of the approaches and strategies to be used in protecting information assets is assigning user IDs that will have these general characteristics”)

---

## KEY ELEMENTS

While policies are related, and as above, can be hierarchical in nature, each policy must be tested separately. Therefore, certain key elements must be included in each.

- 1) **ID:** Title of policy topic must be clearly defined by a unique title
- 2) **TOPIC (PURPOSE):** business value, business risk and goal of policy must be clear
- 3) **SCOPE (RELEVANCE):** Who/what will this policy apply to? Scope must be clear and bounded, devoid of ambiguities
- 4) **RESPONSIBILITIES:** What job roles are responsible for carrying out the policies
- 5) **COMPLIANCE:** What constitutes deviation or violation, and what penalties will be applied in such case.
- 6) **OPTIONAL:**
  - a. **DEFINITIONS:** include these for any unusual term or phrase
  - b. **STANDARDS** and **PROCEDURES**
  - c. **TOOLS**
  - d. **EXCEPTIONS**
  - e. **PROVISIONS**
  - f. **OTHER**



## RECOMMENDED APPROACH

- a) Check to make sure no other existing policy covers the topic
- b) Check to make sure all Key Elements (non-optional) are present
- c) Make sure all affected roles are included and that the Scope and Purpose is worded broadly enough to cover all of them.
- d) Check (especially Scope) for wishy-washy phrases like “includes, but is not limited to...”
- e) Make sure Responsibilities includes the role accountable for policy enforcement.
- f) Where reasonable, include examples of unacceptable behavior, and be clear about the company’s position on the consequences of non-compliance.
- g) Check for internal consistency.
- h) Check for conflicts with other policies, especially related to timing. Oftentimes, related policies are really dependents or pre-requisites of others. As yourself, if a policy were used used without knowledge or pre-execution of its related policies, could a misinterpretation occur?
- i) Focus on clarity of expression. Could this policy be misinterpreted?



## Sample Policies

### Access Control Policy—Program Level

ID: Access Control

#### MANDATORY ELEMENTS

- ✓ Topic
- ✓ Scope
- ✓ Responsibilities
- ✓ Compliance

**Topic (Purpose):** Business information is the organization's core commodity and represents the bulk of the business value of the company. Whether in electronic, handwritten or printed form, whether stored in active or backup tapes, contained in onsite servers and workstations, or on laptops or hand held devices, information concerning the company's business and customers must be protected. Without such protection, our company's ability to meet its commitments to its customers, business partners and employees can be significantly impaired.

#### Scope (Relevance)

This policy applies to all employees and temporary employees of the company and governs all information created or housed by the company.

#### Employee Responsibilities

All company employees are expected to exercise prudent judgment in the use of company computer property and in the handling of company information, regardless of its sensitivity levels.

Management is responsible for ensuring that all employees understand their obligations to protect these assets, and that new hires are appropriately screened and orientated.

Operations Personnel who are granted broad access rights are expected to exercise restraint in their use and to use such rights only for the specified administrative purpose.

Details of each employee's responsibilities according to job role are documented in the Information Protection Policies and Standards manual.

#### Compliance

The CIO is responsible for the monitoring and enforcement of this policy. Violations to Company procedures outlined in the Policies and Standards manual are serious, and are subject to appropriate disciplinary action up to an including discharge, legal action and referring the matter to law enforcement. Human resource Policy Guide for Management will be referenced in the event of a suspected violation.



## Access Control—Topic –Specific Policy

**ID: User Access Management**

### Topic (Purpose)

Unauthorized access to information represents a serious threat to the organization. To ensure against accidental exposure of information and to limit the opportunity for malicious use, access to information systems will be controlled.

#### MANDATORY ELEMENTS

- √ Topic
- √ Scope
- √ Responsibilities
- √ Compliance

**Scope (Relevance):** This policy applies to anyone who has a need to access data from company computers.

### Definitions:

“Least privilege” is the principle whereby users are granted access to only as many resources and as much data as is needed to accomplish their job role duties.

### Responsibilities

Management is responsible for applying for and approving access to specific resources for persons under their charge, and limiting access to resources and information based on job role. Managers are responsible for informing User Access Administrators of any change to an employee’s job role, including termination, where immediate revocation of rights is expected.

HR is responsible for notifying Access Administrators immediately of any substantiated security complaint lodged against an employee, or of any employee pending termination so that preparations can be made for revocation of rights on demand.

User Access Administrators are responsible for allocating, managing, de-registering and destroying User IDs when needed, and according to standards and procedures defined in the Access Management manual, or under emergency circumstances, when and as required by Senior management. They are responsible for providing periodic reports to each manager so they can check to ensure access is current and appropriate for their employees.

Users are responsible for the protecting their User IDs and associated passwords, which includes never sharing them or allowing anyone to obtain them, and reporting accidental disclosure immediately to their direct supervisor or a security authority.

Senior management is responsible for communicating any changes to this policy promptly to all affected parties.

**Compliance:** The Risk Management Department is responsible for the monitoring and enforcement of this policy. Penalties for non-compliance with this policy can be severe, resulting in administrative action, suspension, loss of job, or reporting to legal authorities or law enforcement if the circumstance is suspected as a deliberate or malicious act.



## Access Control—Technology-Specific Policy

**ID:** Password Threshold Reset

### MANDATORY ELEMENTS

- ✓ Topic
- ✓ Scope
- ✓ Responsibilities
- ✓ Compliance

**Topic (Purpose)** Computer system access controls can be compromised using automated tools that “guess” passwords. To impede this activity, and to help detect such malicious attacks, a password reset threshold must be set.

**Scope (Relevance):** Thresholds will be applied to all company computer systems, except those used in the test lab.

### Responsibilities:

System administrators are responsible for activating thresholds for each required system and formalizing the administrative procedure that enables the employee to recover their id and password in a safe manner.

Education and Training personnel will ensure employees are aware of this policy and the reset request procedure.

Managers are responsible for ensuring that System Administrators follow a checklist when implementing or changing system/network access configuration to ensure the setting of password access.

**Standards:**

- 1) All systems will lock out ID attempts after three tries
- 2) Access will be automatically restored after 30 minutes.
- 3) All password resets must show clear audit trail

**Exceptions:** If recovery is required in less than 30 minutes, user mgt. authorization is required.

### Procedure:

- a) Thresholds will be set by following the Standard Access Controls Procedures.
- b) If management does not authorize manual script run to recover passwords prior to 30 minutes, user should be informed to wait 30 minutes.
- c) If management does authorize manual script run, Administrator should check with Admin Mgt. to ensure the activity does not interfere with higher priority tasks. If the activity will be delayed, User Management should be informed.
- d) If manual script run takes place, the activity must be manually logged as a workorder, and a trouble ticket (if not already in process) should be created and resolved.

**Tools:** Script A is used for manual recovery



**Compliance:** Non-compliance can enable the opportunity for a denial of service attack on the system, and increases the possibility of unauthorized access. System Administration Management is responsible for the enforcement of this policy. Audit will periodically spot check access ids for adherence to protocol. Reported violations will be considered dereliction of job role duties, subject to Senior Management review.