UTeM

اونيۏرسيتي تيکنيکل مليسيا ملاک

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Always A Pioneer, Always Ahead

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UTeM

MyUTeM

BITS 2523
Cyberlaw & Security Policy
Lecture 12

By

Mohd Fairuz Iskandar Othman, Phd

mohdfairuz@utem.edu.my

Security Policy Model Part 1

Topics covered:

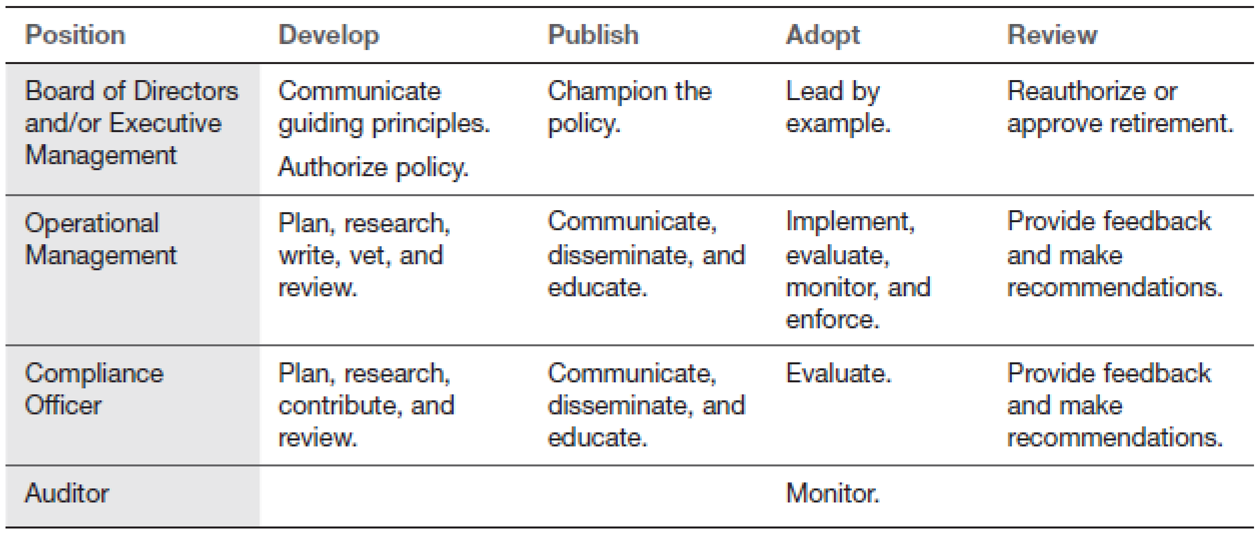
- Information Security Policy Lifecycle
- Policy Hierarchy
- Policy Format
- Writing style and technique

Information Security Policy Lifecycle

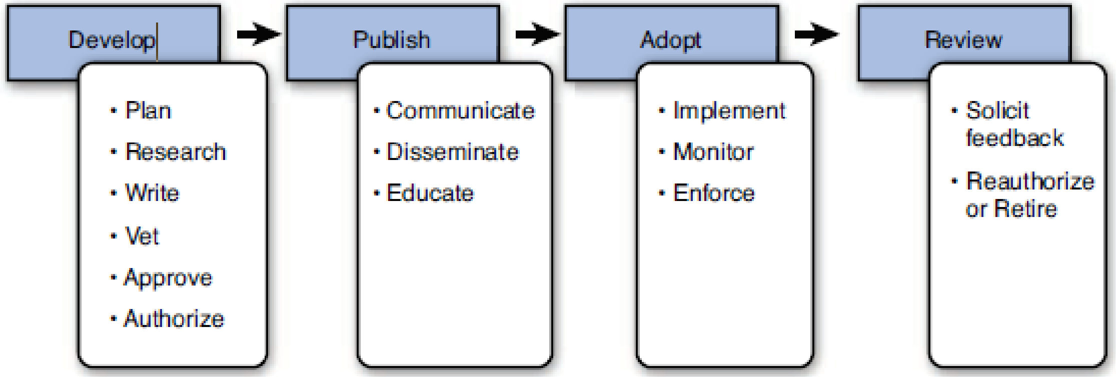
- Regardless of whether a policy is based on guiding principles or regulatory requirements, its success depends in large part upon how the organization approaches the tasks of policy development, publication, adoption, and review.
- Collectively, this process is referred to as the policy lifecycle, as illustrated in Figure 1.2. The responsibilities associated with the policy lifecycle process are distributed throughout an organization as outlined in Table 1.1.
- Organizations that understand the lifecycle and take a structured approach will have a much better chance of success.
- The objective of this section is to introduce you to the components that make up the policy lifecycle. Throughout the text, we will examine the process as it relates to specific information security policies.

Information Security Policy Lifecycle

TABLE 1.1 Information Security Policy Lifecycle Responsibilities



Position	Develop	Publish	Adopt	Review
Board of Directors and/or Executive Management	Communicate guiding principles. Authorize policy.	Champion the policy.	Lead by example.	Reauthorize or approve retirement.
Operational Management	Plan, research, write, vet, and review.	Communicate, disseminate, and educate.	Implement, evaluate, monitor, and enforce.	Provide feedback and make recommendations.
Compliance Officer	Plan, research, contribute, and review.	Communicate, disseminate, and educate.	Evaluate.	Provide feedback and make recommendations.
Auditor			Monitor.	



Develop
- Plan
- Research
- Write
- Vet
- Approve
- Authorize

Publish
- Communicate
- Disseminate
- Educate

Adopt
- Implement
- Monitor
- Enforce

Review
- Solicit feedback
- Reauthorize or Retire

FIGURE 1.2 Information security policy lifecycle.

Information Security Policy Lifecycle

Policy Development

- Even before setting pen to paper, considerable thought and effort need to be put into developing a policy. Once the policy is written, it still needs to go through an extensive review and approval process.
- There are six key tasks in the development phase: planning, researching, writing, vetting, approving, and authorizing.

1. The seminal planning task should identify the need for and context of the policy. Policies should never be developed for their own sake. There should always be a reason. Polices may be needed to support business objectives, contractual obligations, or regulatory requirements. The context could vary from the entire organization to a specific subset of users.
2. Policies should support and be in agreement with relevant laws, obligations, and customs. The research task focuses on defining operational, legal, regulatory, or contractual requirements and aligning the policy with the aforementioned. This objective may sound simple, but in reality is extremely complex. Some regulations and contracts have very specific requirements whereas others are extraordinarily vague. Even worse, they may contradict each other.

Information Security Policy Lifecycle

Policy Development

3. In order to be effective, policies must be written for their intended audience. Language is powerful and is arguably one of the most important factors in gaining acceptance and, ultimately, successful implementation. The writing task requires that the audience is identified.
4. Policies require scrutiny. The vetting task requires the authors to consult with internal and external experts, including legal counsel, human resources, compliance, information security and technology professionals, auditors, and regulators.
5. Because information security policies affect an entire organization, they are inherently cross departmental. The approval task requires that the authors build consensus and support. All affected departments should have the opportunity to contribute to, review, and, if necessary, challenge the policy before it is authorized. Within each department, key people should be identified, sought out, and included in the process. Involving them will contribute to the inclusiveness of the policy and, more importantly, may provide the incentive for them to champion the policy.
6. The authorization task requires that executive management or an equivalent authoritative body agree to the policy. Generally, the authority has oversight responsibilities and can be held legally liable. Both GLBA and HIPAA require written information security policies that are Board-approved and subject to at least annual review. Boards of Directors are often composed of experienced albeit nontechnical business people from a spectrum of industry sectors. It is helpful to know who the Board members are, and their level of understanding, so that policies are presented in a meaningful way.

Information Security Policy Lifecycle

Policy Publication

- Once you have the "green light" from the authority, it is time to publish and introduce the policy to the organization as a whole. This introduction will require careful planning and execution because it will set the stage for how well the policy is accepted and followed. There are three key tasks in the publication phase: communication, dissemination, and education.

  1. The objective of the communication task is to deliver the message that the policy or policies are important to the organization. In order to accomplish this task, visible leadership is required. There are two very distinct types of leaders in the world: those who see leadership as a responsibility and those who see it as a privilege.
  2. Disseminating the policy simply means making it available. Although the task seems obvious, it is mind boggling how many organizations store their policies in locations that make them, at best, difficult to locate and, at worst, totally inaccessible. Policies should be widely distributed and available to their intended audience. This does not mean that all polices should be available to everyone because there may be times when certain polices contain confidential information that should only be made available on a restricted or need-to-know basis.
  3. Companywide training and education build culture. When people share experiences, they are drawn together; they can reinforce one another's understanding of the subject matter and therefore support whatever initiative the training was intended to introduce. Introducing information security policies should be thought of as a teaching opportunity with the goal of raising awareness, and giving each person a tangible connection to the policy objective. Initial education should be coupled with ongoing awareness programs designed to reinforce the importance of policy-driven security practices.

Information Security Policy Lifecycle

Policy Publication

- Multiple factors contribute to an individual's decision to comply with a rule, policy, or law, including the chance of being caught, the reward for taking the risk, and the consequences. Organizations can influence individual decision making by creating direct links between individual actions, policy, and success.
- Creating a culture of compliance means that each participant not only recognizes and understands the purpose of a policy, they also actively look for ways to champion the policy. Championing a policy means being willing to demonstrate visible leadership and to encourage and educate others. Creating a culture of information security policy compliance requires an ongoing investment in training and education, measurements, and feedback.

Information Security Policy Lifecycle

Policy Adoption

- The policy has been announced and the reasons communicated. Now the hard work of adoption starts. Successful adoption begins with an announcement, progresses through implementation, performance evaluation, and process improvement, with the ultimate goal being normative integration. For our purposes, normative integration means that the policy and corresponding implementation is expected behavior—all others being deviant. There are three key tasks in the adoption phase: implementation, monitoring, and enforcement:

1. Implementation is the busiest and most challenging task of all. The starting point is ensuring that everyone involved understands the intent of the policy as well as how it is to be applied. Decisions may need to be made regarding the purchase and configuration of supporting administrative, physical, and technical controls. Capital investments may be need to be budgeted for. A project plan may need to be developed and resources assigned. Management and affected personnel need to be kept informed. Situations where implementation is not possible need to be managed, including a process for granting either temporary or permanent exceptions.
2. Post-implementation, compliance and policy effectiveness need to be monitored and reported. Mechanisms to monitor compliance range from application-generated metrics to manual audits, surveys, and interviews as well as violation and incident reports.
3. Unless there is an approved exception, policies must be enforced consistently and uniformly. The same is true of violation consequences. If a policy is enforced only for certain circumstances and people, or if enforcement depends on which supervisor or manager is in charge, eventually there will be adverse consequences. Once there is talk within an organization that different standards for enforcement exist, the organization is open to many cultural problems, the most severe of which involve discrimination lawsuits.

Information Security Policy Lifecycle

Policy Review

- Change is inherent in every organization. Policies must support the guiding principles, organizational goals, and forward-facing initiatives. They must also be harmonized with regulatory requirements and contractual obligations. The two key tasks in the review phase are soliciting feedback and reauthorizing or retiring policies:
  1. Continuing acceptance of information security policies hinges on making sure the policies keep up with significant changes in the organization or the technology infrastructure. Policies should be reviewed annually. Similar to the development phase, feedback should be solicited from internal and external sources.
  2. Policies that are outdated should be refreshed. Policies that are no longer applicable should be retired. Both tasks are important to the overall perception of the importance and applicability of organizational directives. The outcome of the annual review should either be policy reauthorization or policy retirement. The final determination belongs with the Board of Directors or equivalent body.

Policy Hierarchy

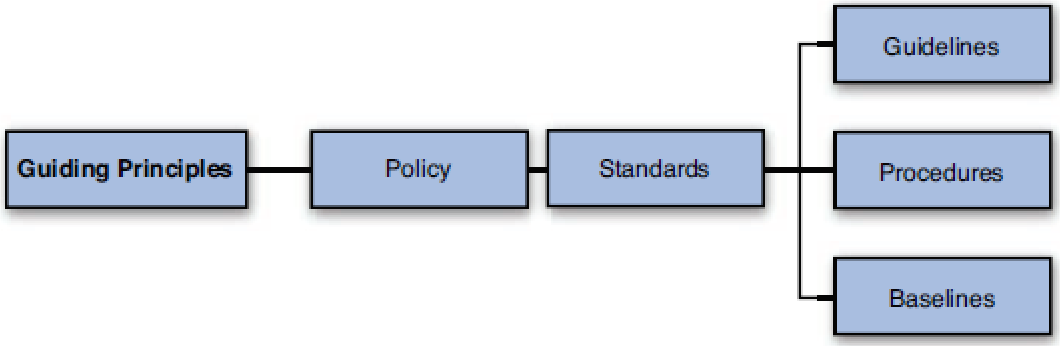


FIGURE 2.1 Policy hierarchy.

Policy Hierarchy

- A policy is a mandatory governance statement that presents management’s position. A well-written policy clearly defines guiding principles, provides guidance to those who must make present and future decisions, and serves as an implementation roadmap.
- Policies are important, but alone they are limited in what they can accomplish. Policies need supporting documents to give them context and meaningful application. Standards, baselines, guidelines, and procedures each play a significant role in ensuring implementation of the governance objective.
- The relationship between the documents is known as the policy hierarchy. In a hierarchy, with the exception of the topmost object, all objects are subordinate to the one above it.
- In a policy hierarchy, the topmost object is the guiding principles, as illustrated in Figure 2.1. Polices reflect the guiding principles and organizational objectives. Standards enable the policies by defining action. Guidelines, procedures, and baselines support the standards.

Policy Hierarchy

Standards

- ***Standards*** serve as specifications for the implementation of policy and dictate mandatory requirements.
- For example, our password policy might simply state the following:
  1. All users must have a unique user ID and password that conforms to the company password standard.
  2. Users must not share their password with anyone regardless of title or position.
  3. If a password is suspected to be compromised, it must be reported immediately to the help desk and a new password must be requested.
- The password standard would then dictate the required password characteristics, such as the following:
  - Minimum of eight upper- and lowercase alphanumeric characters
  - Must include at least one special character (such as *, &, $, #, !, or @)
  - Must not include the user’s name, the company name, or office location
  - Must not include repeating characters (for example, 111)
- The policy represents expectations that are not necessarily subject to changes in technology, processes, or management. The standard, however, is very specific to the infrastructure.
- Standards are determined by management, and unlike policies, they are not subject to Board of Directors authorization. Standards can be changed by management as long as they conform to the intent of the policy.

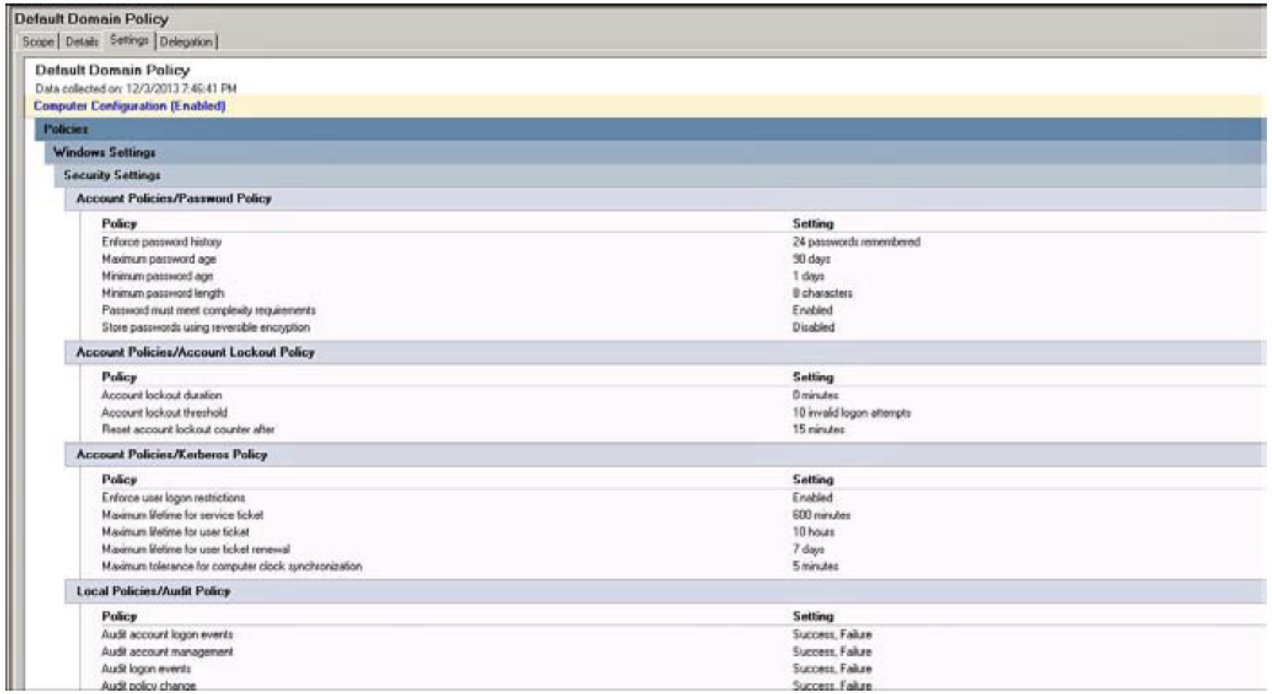
Policy Hierarchy

Baselines

- ***Baselines*** are an aggregate of implementation standards and security controls for a specific category or grouping, such as platform (for example, Windows OS), device type (for example, iPad), ownership (for example, employee owned), and location (for example, mobile users).
- The primary objective of a baseline is uniformity and consistency.
- An example of a baseline related to our password policy and standard example is the mandate that a specific Active Directory Group Policy configuration be used on all Windows devices to technically enforce security requirements, as illustrated in Figure 2.2.
- In this example, by applying the same Active Directory Group Policy to all Windows workstations and servers, the standard was implemented throughout the organization. In this case, there is also assurance that new devices will be configured accordingly.

Policy Hierarchy

Baselines



Default Domain Policy

Scope | Details | Settings | Delegation

Default Domain Policy

Data collected on: 12/3/2013 7:46:41 PM

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	0 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit policy change	Success, Failure

FIGURE 2.2 Windows Group Policy settings.

Policy Hierarchy

Guidelines

- ***Guidelines*** are best thought of as teaching tools. The objective of a guideline is to help people conform to a standard. In addition to using softer language than standards, guidelines are customized for the intended audience and are not mandatory. Guidelines are akin to suggestions or advice. A guideline related to the password standard in the previous example might read like this:

"A good way to create a strong password is to think of a phrase, song title, or other group of words that is easy to remember and then convert it, like this:

    - "The phrase 'Up and at 'em at 7!' can be converted into a strong password such as **up&atm@7!**.
    - "You can create many passwords from this one phrase by changing the number, moving the symbols, or changing the punctuation mark."

- This guideline is intended to help readers create easy-to-remember, yet strong passwords.

Policy Hierarchy

Procedures

- ***Procedures*** are instructions for how a policy, standard, baseline, and guidelines are carried out in a given situation. Procedures focus on actions or steps, with a specific starting and ending point. There are four commonly used procedure formats:
  - **Simple Step**—Lists sequential actions. There is no decision making.
  - **Hierarchical**—Includes both generalized instructions for experienced users and detailed instructions for novices.
  - **Graphic**—This format uses either pictures or symbols to illustrate the step.
  - **Flowchart**—Used when a decision-making process associated is with the task.
- In keeping with our previous password example, let's take a look at a Simple Step procedure for changing a user's Windows password:
  1. Press and hold the Ctrl+Alt+Delete keys.
  2. Click the Change Password option.
  3. Type your current password in the top box.
  4. Type your new password in both the second and third boxes. (If the passwords don't match, you will be prompted to reenter your new password.)
  5. Click OK and then log in with your new password.

Policy Hierarchy

Plans and Programs

- The function of a plan is to provide strategic and tactical instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain timeframe, usually with defined stages and with designated resources. Plans are sometimes referred to as programs. For our purposes, the terms are interchangeable. Here are some examples of information security–related plans :
  - Vendor Management Plan
  - Incident Response Plan
  - Business Continuity Plan
  - Disaster Recovery Plan
- Policies and plans are closely related. For example, an Incident Response Policy will generally include the requirement to publish, maintain, and test an Incident Response Plan. Conversely, the Incident Response Plan gets its authority from the policy.
- Quite often, the policy will be included in the plan document.

Policy Format

- Writing policy documents can be challenging. Polices are complex documents that must be written to withstand legal and regulatory scrutiny while at the same time be easily read and understood by the reader. The starting point for choosing a format is identifying the policy audience.

Policy Audience

- Who the policy is intended for is referred to as the ***policy audience***. It is imperative, during the planning portion of the security policy project, to clearly define the audience. Policies may be intended for a particular group of employees based on job function or role. An application development policy is targeted to developers. Other policies may be intended for a particular group or individual based on organizational role, such as a policy defining the responsibility of the Information Security Officer.
- The policy, or portions of it, can sometimes apply to people outside of the company, such as business partners, service providers, contractors, or consultants. The policy audience is a potential resource during the entire policy lifecycle. Indeed, who better to help create and maintain an effective policy than the very people whose job it is to use those policies in the context of their everyday work?

Policy Format

Policy Format Types

- Organize, before you begin writing! It is important to decide how many sections and subsections you will require before you put pen to paper. Designing a template that allows the flexibility of editing will save considerable time and reduce aggravation.
- There are two schools of thought in regard to policy format. The first is to write each policy as a discrete document; this document type is referred to as a singular policy. The second is to group like policies together; this document type is referred to as a consolidated policy. Consolidated policies are often organized by section and subsection. Table 2.1 illustrates policy document format options.

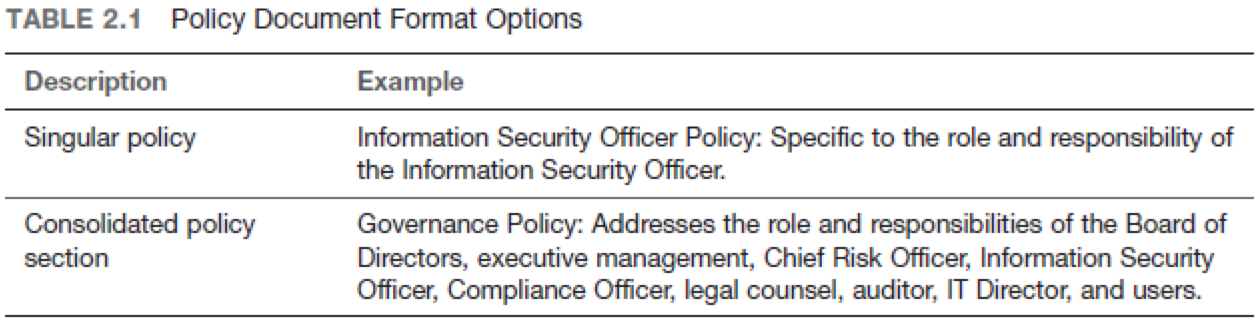


TABLE 2.1 Policy Document Format Options

Description	Example
Singular policy	Information Security Officer Policy: Specific to the role and responsibility of the Information Security Officer.
Consolidated policy section	Governance Policy: Addresses the role and responsibilities of the Board of Directors, executive management, Chief Risk Officer, Information Security Officer, Compliance Officer, legal counsel, auditor, IT Director, and users.

Policy Format

Policy Format Types

- The advantage to individual policies is that each policy document can be short, clean and crisp, and targeted to its intended audience.
- The disadvantage is the need to manage multiple policy documents and the chance that they will become fragmented and lose consistency.
- The advantage to consolidation is that it presents a composite management statement in a single voice.
- The disadvantage is the potential size of the document and the reader challenge of locating applicable sections.
- For many organizations, managing singular policies has become unwieldy. The current trend is toward consolidation.
- Regardless of which format you choose, do not include standards, baselines, guidelines, or procedures in your policy document.

Policy Format

Policy Format Types

- If you do so, you will end up with one big unruly document. You will undoubtedly encounter one or more of the following problems:
  - **Management challenge**—Who is responsible for managing and maintaining a document that has multiple contributors?
  - **Difficulty of updating**—Because standards, guidelines, and procedures change far more often than policies, updating this whale of a document will be far more difficult than if these elements were properly treated separately. Version control will become a nightmare.
  - **Cumbersome approval process**—Various regulations as well as the Corporate Operating Agreement require that the Board of Directors approve new policies as well as changes. Mashing it all together means that every change to a procedure, guideline, or standard will potentially require the Board to review and approve. This will become very costly and cumbersome for everyone involved.

Policy Format

Policy Components

- Policy documents have multiple sections or components (see Table 2.2). How the components are used and in what order will depend on which format—singular or consolidated—you choose.

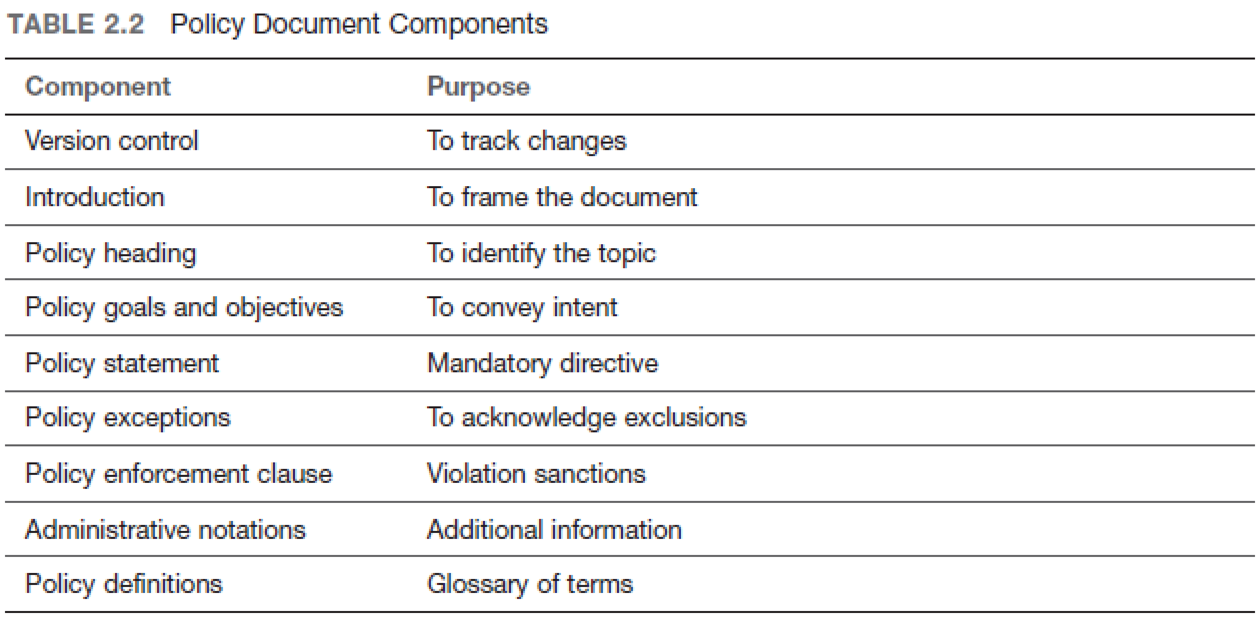


TABLE 2.2 Policy Document Components

Component	Purpose
Version control	To track changes
Introduction	To frame the document
Policy heading	To identify the topic
Policy goals and objectives	To convey intent
Policy statement	Mandatory directive
Policy exceptions	To acknowledge exclusions
Policy enforcement clause	Violation sanctions
Administrative notations	Additional information
Policy definitions	Glossary of terms

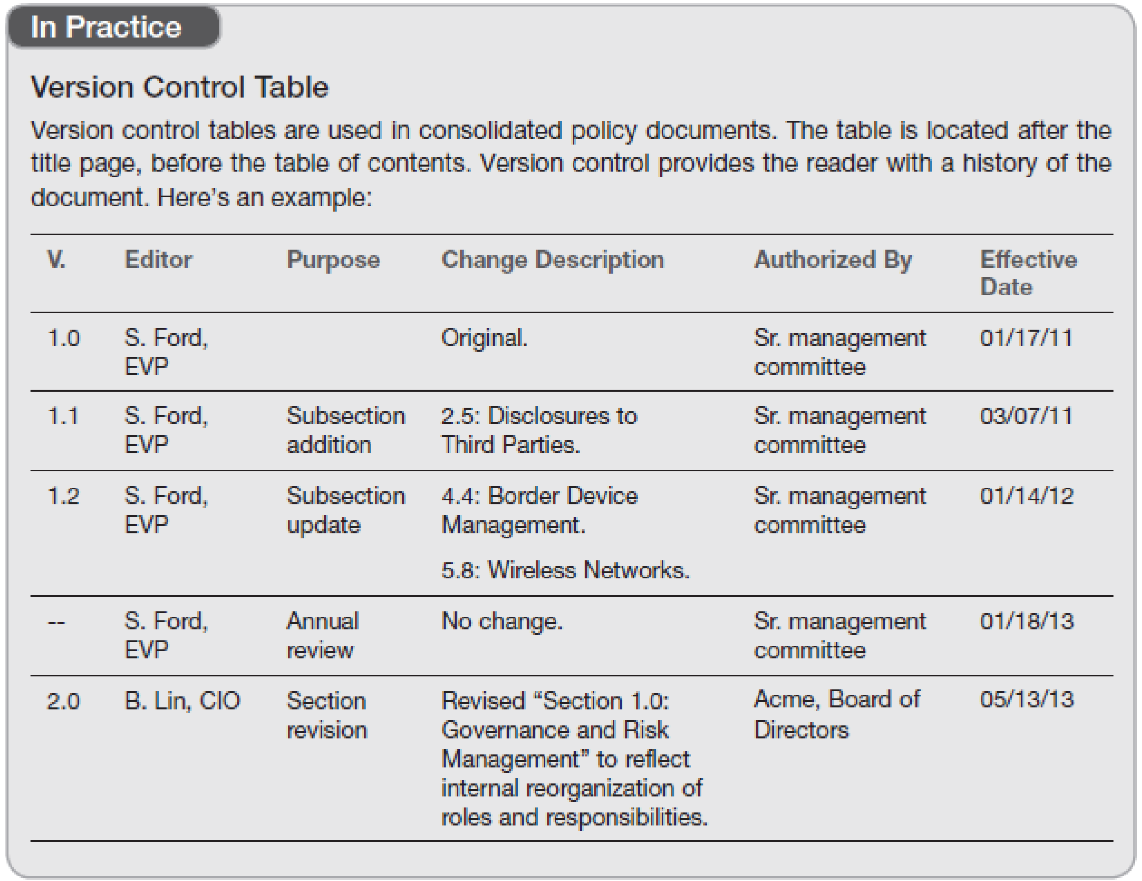
Policy Format

Version Control

- Best practices dictate that policies are reviewed annually to ensure they are still applicable and accurate. Of course, policies can (and should) be updated whenever there is a relevant change driver.
- Version control, as it relates to policies, is the management of changes to the document. Versions are usually identified by a number or letter code. Major revisions generally advance to the next letter or digit (for example, from 2.0 to 3.0). Minor revisions generally advance as a subsection (for example, from 2.0 to 2.1).
- Version control documentation should include the change date, name of the person or persons making the change, a brief synopsis of the change, the name of the person, committee, or board that authorized the change, and the effective date of the change.
  - For singular policy documents, this information is split between the policy heading and the administrative notation sections.
  - For consolidated policy documents, a version control table is included either at the beginning of the document or at the beginning of a section.

Policy Format

Version Control



In Practice

Version Control Table

Version control tables are used in consolidated policy documents. The table is located after the title page, before the table of contents. Version control provides the reader with a history of the document. Here's an example:

V.	Editor	Purpose	Change Description	Authorized By	Effective Date
1.0	S. Ford, EVP		Original.	Sr. management committee	01/17/11
1.1	S. Ford, EVP	Subsection addition	2.5: Disclosures to Third Parties.	Sr. management committee	03/07/11
1.2	S. Ford, EVP	Subsection update	4.4: Border Device Management. 5.8: Wireless Networks.	Sr. management committee	01/14/12
--	S. Ford, EVP	Annual review	No change.	Sr. management committee	01/18/13
2.0	B. Lin, CIO	Section revision	Revised "Section 1.0: Governance and Risk Management" to reflect internal reorganization of roles and responsibilities.	Acme, Board of Directors	05/13/13

Policy Format

Introduction

- This is where we first meet the reader and have the opportunity to engage them. Here are the objectives of the introduction:
  - To provide context and meaning
  - To convey the importance of understanding
  - To acquaint the reader with the document and its contents
  - To explain the exemption process as well as the consequence of noncompliance
  - To thank the reader and to reinforce the authority of the policyand adhering to the policy
- The first part of the introduction should make the case for why policies are necessary. It is a reflection of the guiding principles, defining for the reader the core values the company believes in and is committed to. This is also the place to set forth the regulatory and contractual obligations that the company has - often by listing which regulations, such as GLBA, HIPAA, or MA CMR 17 201, pertain to the organization as well as the scope of the policy.
- The second part of the introduction should leave no doubt that compliance is mandatory. A strong statement of expectation from a senior authority such as the Chairman of the Board, CEO, or President is appropriate. Readers should understand that they are unequivocally and directly responsible for the safeguarding of information and systems in the course of their normal employment or relationship with the company. It should also make clear that questions are welcome and a resource is available who can clarify the policy and/or assist with compliance.

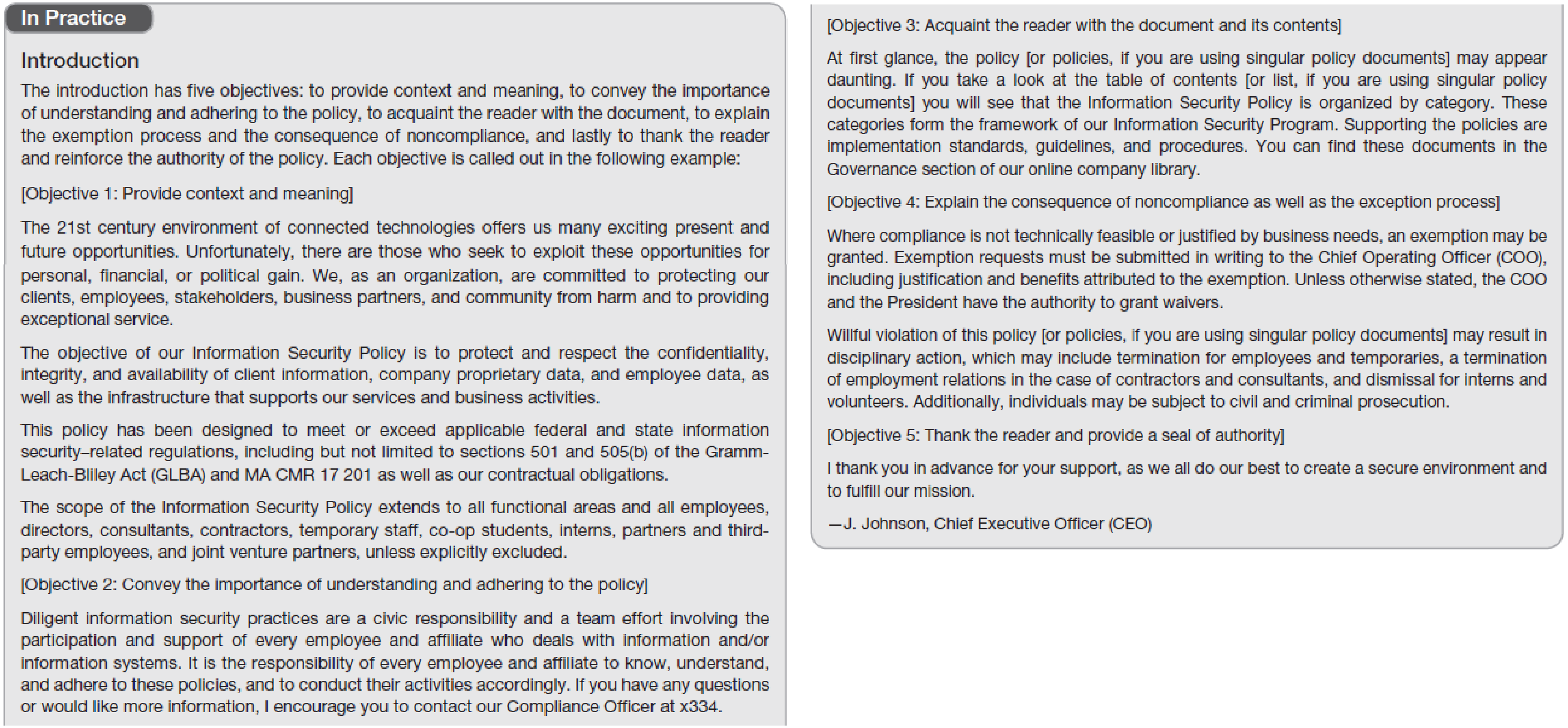
Policy Format

Introduction

- The third part of the introduction should describe the policy document, including the structure, categories, and storage location (for example, the company intranet). It should also reference companion documents such as standards, guidelines, programs, and plans.
- The fourth part of the introduction should explain how to handle situations where compliance may not be feasible. It should explain the exemption process. The section should also address the consequences of willful noncompliance.
- The introduction should end with a "thank you" and with words of encouragement. The introduction should be signed by a person who has the authority to enforce the policy. This final statement reinforces the organizational commitment.
    - For singular policy documents, the introduction should be a separate document.
    - For consolidated policy documents, the introduction serves as the preface and follows the version control table.

Policy Format

Introduction



In Practice

Introduction

The introduction has five objectives: to provide context and meaning, to convey the importance of understanding and adhering to the policy, to acquaint the reader with the document, to explain the exemption process and the consequence of noncompliance, and lastly to thank the reader and reinforce the authority of the policy. Each objective is called out in the following example:

[Objective 1: Provide context and meaning]

The 21st century environment of connected technologies offers us many exciting present and future opportunities. Unfortunately, there are those who seek to exploit these opportunities for personal, financial, or political gain. We, as an organization, are committed to protecting our clients, employees, stakeholders, business partners, and community from harm and to providing exceptional service.

The objective of our Information Security Policy is to protect and respect the confidentiality, integrity, and availability of client information, company proprietary data, and employee data, as well as the infrastructure that supports our services and business activities.

This policy has been designed to meet or exceed applicable federal and state information security–related regulations, including but not limited to sections 501 and 505(b) of the Gramm-Leach-Bliley Act (GLBA) and MA CMR 17 201 as well as our contractual obligations.

The scope of the Information Security Policy extends to all functional areas and all employees, directors, consultants, contractors, temporary staff, co-op students, interns, partners and third-party employees, and joint venture partners, unless explicitly excluded.

[Objective 2: Convey the importance of understanding and adhering to the policy]

Diligent information security practices are a civic responsibility and a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee and affiliate to know, understand, and adhere to these policies, and to conduct their activities accordingly. If you have any questions or would like more information, I encourage you to contact our Compliance Officer at x334.

[Objective 3: Acquaint the reader with the document and its contents]

At first glance, the policy [or policies, if you are using singular policy documents] may appear daunting. If you take a look at the table of contents [or list, if you are using singular policy documents] you will see that the Information Security Policy is organized by category. These categories form the framework of our Information Security Program. Supporting the policies are implementation standards, guidelines, and procedures. You can find these documents in the Governance section of our online company library.

[Objective 4: Explain the consequence of noncompliance as well as the exception process]

Where compliance is not technically feasible or justified by business needs, an exemption may be granted. Exemption requests must be submitted in writing to the Chief Operating Officer (COO), including justification and benefits attributed to the exemption. Unless otherwise stated, the COO and the President have the authority to grant waivers.

Willful violation of this policy [or policies, if you are using singular policy documents] may result in disciplinary action, which may include termination for employees and temporaries, a termination of employment relations in the case of contractors and consultants, and dismissal for interns and volunteers. Additionally, individuals may be subject to civil and criminal prosecution.

[Objective 5: Thank the reader and provide a seal of authority]

I thank you in advance for your support, as we all do our best to create a secure environment and to fulfill our mission.

—J. Johnson, Chief Executive Officer (CEO)

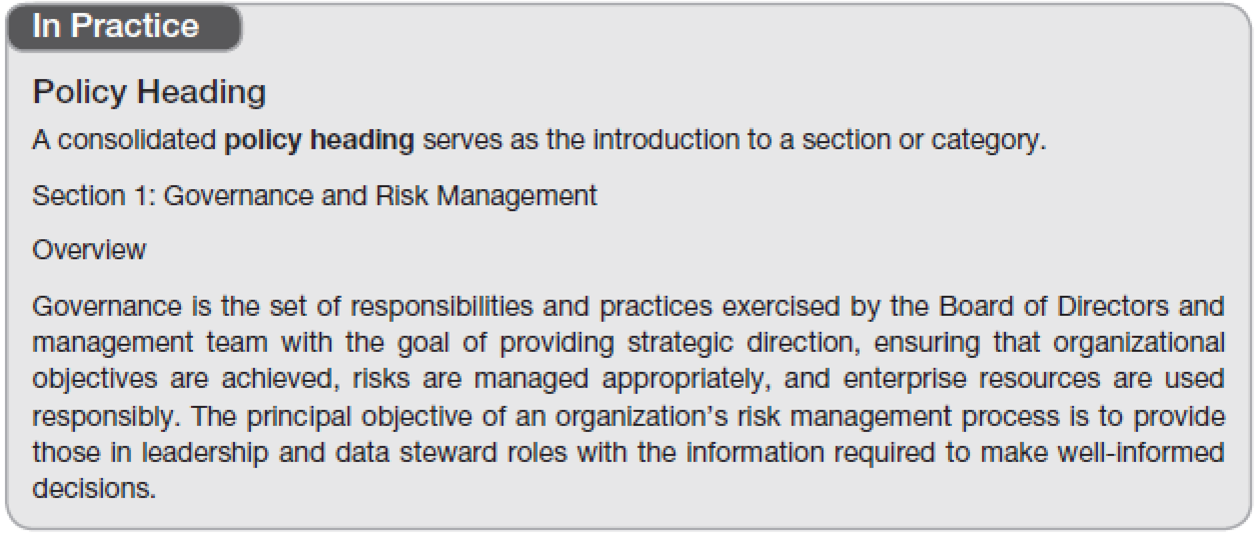
Policy Format

Policy Heading

- A policy heading identifies the policy by name and provides the reader with an overview of the policy topic or category. The format and contents of the heading significantly depend on the format (singular or consolidated) you are using.
  - Singular policies must be able to stand on their own, which means it is necessary to include significant logistical detail in each heading. The information contained in a singular policy heading may include the organization or division name, category (section), subsection, policy number, name of the author, version number, approval authority, effective date of the policy, regulatory cross-reference, and a list of supporting resources and source material. The topic is generally self-explanatory and does not require an overview or explanation.
  - In a consolidated policy document, the heading serves as a section introduction and includes an overview. Because the version number, approval authority, and effective date of the policy have been documented in the version control table, it is unnecessary to include them in section headings. Regulatory cross-reference (if applicable), lead author, and supporting documentation are found in the Administrative Notation section of the policy.

Policy Format

Policy Heading



In Practice

Policy Heading

A consolidated **policy heading** serves as the introduction to a section or category.

Section 1: Governance and Risk Management

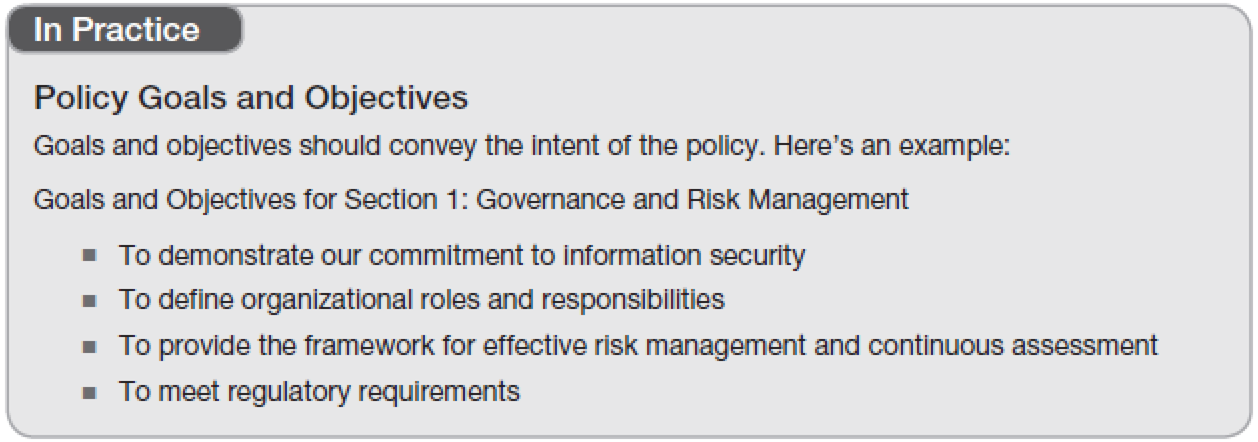
Overview

Governance is the set of responsibilities and practices exercised by the Board of Directors and management team with the goal of providing strategic direction, ensuring that organizational objectives are achieved, risks are managed appropriately, and enterprise resources are used responsibly. The principal objective of an organization's risk management process is to provide those in leadership and data steward roles with the information required to make well-informed decisions.

Policy Format

Policy Goals and Objectives

- Policy goals and objectives act as a gateway to the content to come and the security principle they address. This component should concisely convey the intent of the policy. Note that even a singular policy can have multiple objectives. We live in a world where business matters are complex and interconnected, which means that a policy with a single objective might risk not covering all aspects of a particular situation. It is therefore important, during the planning phase, to pay appropriate attention to the different objectives the security policy should seek to achieve.
  - Singular policies list the goals and objectives either in the policy heading or in the body of the document.
  - In a consolidated policy document, the goals and objectives are grouped and follow the policy heading.



In Practice

Policy Goals and Objectives

Goals and objectives should convey the intent of the policy. Here’s an example:

Goals and Objectives for Section 1: Governance and Risk Management

- To demonstrate our commitment to information security
- To define organizational roles and responsibilities
- To provide the framework for effective risk management and continuous assessment
- To meet regulatory requirements

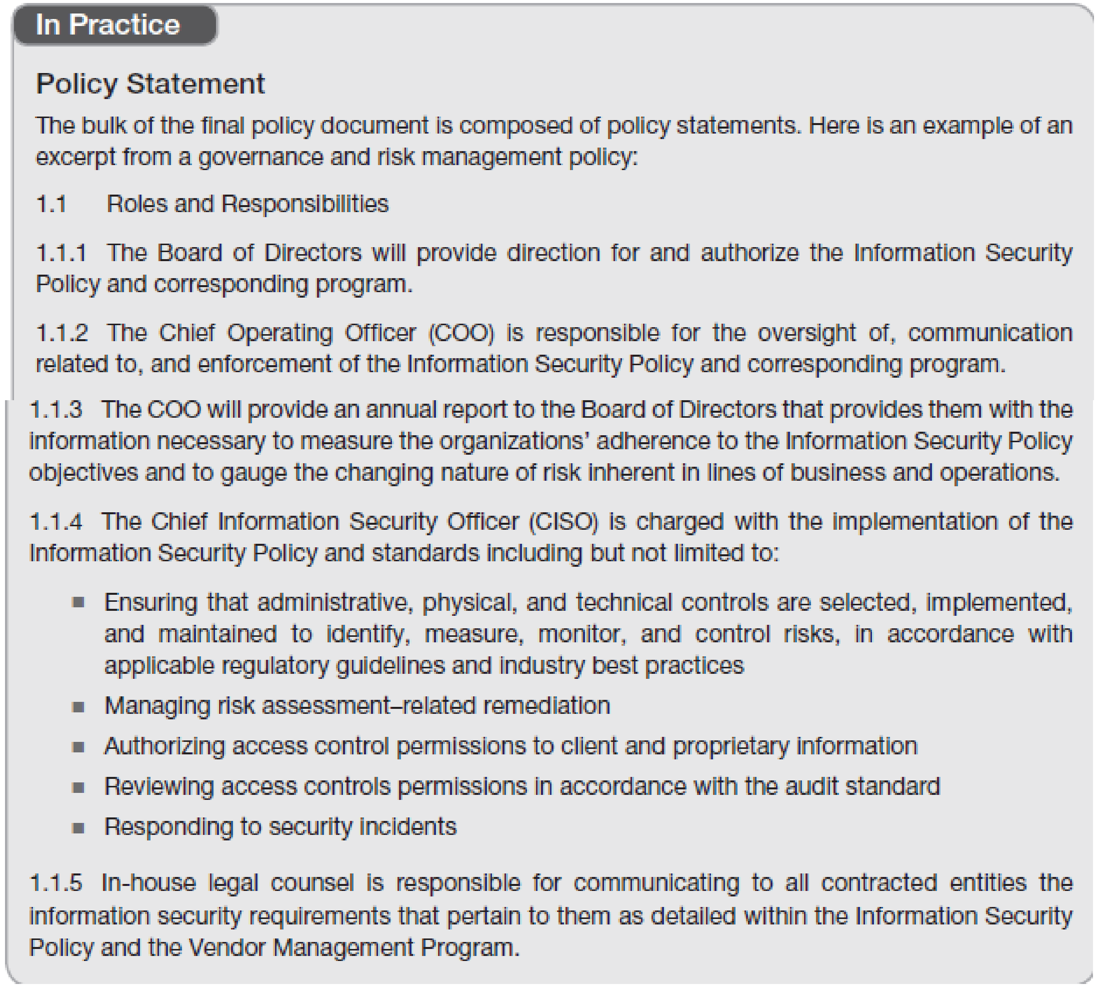
Policy Format

Policy Statement

- Up to this point in the document, we have discussed everything but the actual policy statement. The policy statement is best thought of as a high-level directive or strategic roadmap.
- This is the section where we lay out the rules that need to be followed and, in some cases, reference the implementation instructions (standards) or corresponding plans.
- Policy statements are intended to provide action items as well as the framework for situational responses. Policies are mandatory. Deviations or exceptions must be subject to a rigorous examination process.

Policy Format

Policy Statement



In Practice

Policy Statement

The bulk of the final policy document is composed of policy statements. Here is an example of an excerpt from a governance and risk management policy:

1.1 Roles and Responsibilities

1.1.1 The Board of Directors will provide direction for and authorize the Information Security Policy and corresponding program.

1.1.2 The Chief Operating Officer (COO) is responsible for the oversight of, communication related to, and enforcement of the Information Security Policy and corresponding program.

1.1.3 The COO will provide an annual report to the Board of Directors that provides them with the information necessary to measure the organizations' adherence to the Information Security Policy objectives and to gauge the changing nature of risk inherent in lines of business and operations.

1.1.4 The Chief Information Security Officer (CISO) is charged with the implementation of the Information Security Policy and standards including but not limited to:

- Ensuring that administrative, physical, and technical controls are selected, implemented, and maintained to identify, measure, monitor, and control risks, in accordance with applicable regulatory guidelines and industry best practices
- Managing risk assessment–related remediation
- Authorizing access control permissions to client and proprietary information
- Reviewing access controls permissions in accordance with the audit standard
- Responding to security incidents

1.1.5 In-house legal counsel is responsible for communicating to all contracted entities the information security requirements that pertain to them as detailed within the Information Security Policy and the Vendor Management Program.

Policy Format

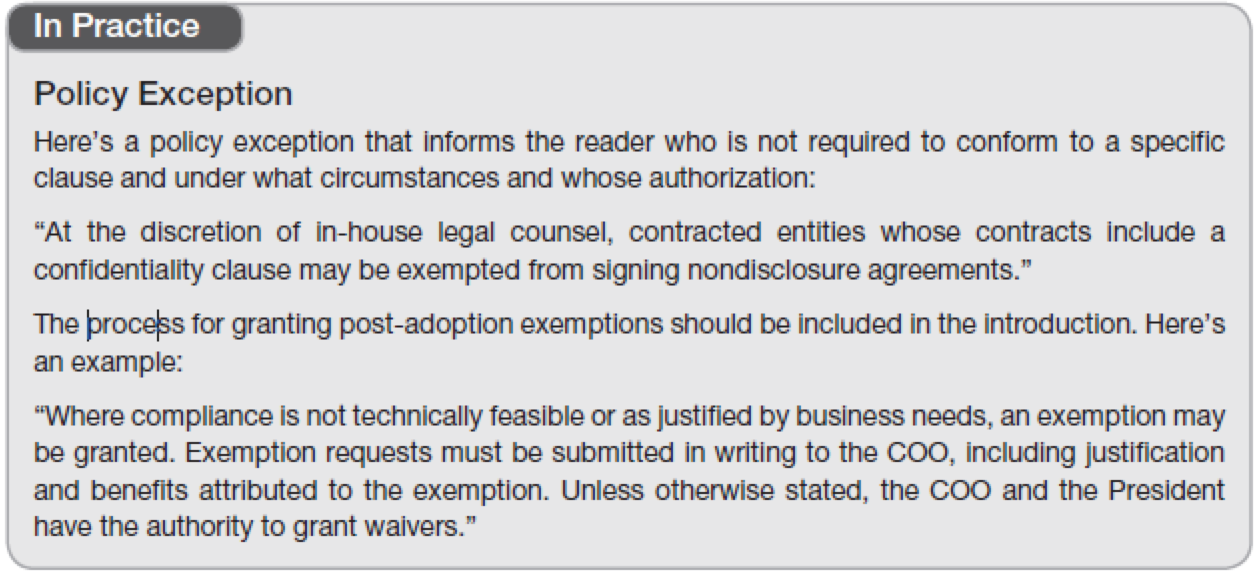
Policy Exceptions and the Exemption Process

- Realistically, there will be situations where it is not possible or practical, or perhaps may even be harmful, to obey a policy directive. This does not invalidate the purpose or quality of the policy. It just means that some special situations will call for exceptions to the rule. Policy exceptions are agreed waivers that are documented within the policy. For example, in order to protect its intellectual property, Company A has a policy that bans digital cameras from all company premises. However, a case could be made that the HR department should be equipped with a digital camera to take pictures of new employees to paste them on their ID badges. Or maybe the Security Officer should have a digital camera to document the proceedings of evidence gathering after a security breach has been detected. Both examples are valid reasons why a digital camera might be needed. In these cases, an exception to the policy could be added to the document. If no exceptions are ever to be allowed, this should be clearly stated in the Policy Statement section as well.
- An **exemption or waiver process is required** for exceptions identified after the policy has been authorized. The exemption process should be explained in the introduction. The criteria or conditions for exemptions should not be detailed in the policy, only the method or process for requesting an exemption. If we try to list all the conditions to which exemptions apply, we risk creating a loophole in the exemption itself. It is also important that the process follow specific criteria under which exemptions are granted or rejected. Whether an exemption is granted or rejected, the requesting party should be given a written report with clear reasons either way.

Policy Format

Policy Exceptions and the Exemption Process

- Finally, it is recommended to keep the number of approved exceptions and exemptions low, for several reasons:
  - Too many built-in exceptions may lead employees to perceive the policy as unimportant.
  - Granting too many exemptions may create the impression of favoritism.
  - Exceptions and exemptions can become difficult to keep track of and successfully audit.
- If there are too many built-in exceptions and/or exemption requests, it may mean that the policy is not appropriate in the first place. At that point, the policy should be subject to review.



In Practice

Policy Exception

Here's a policy exception that informs the reader who is not required to conform to a specific clause and under what circumstances and whose authorization:

"At the discretion of in-house legal counsel, contracted entities whose contracts include a confidentiality clause may be exempted from signing nondisclosure agreements."

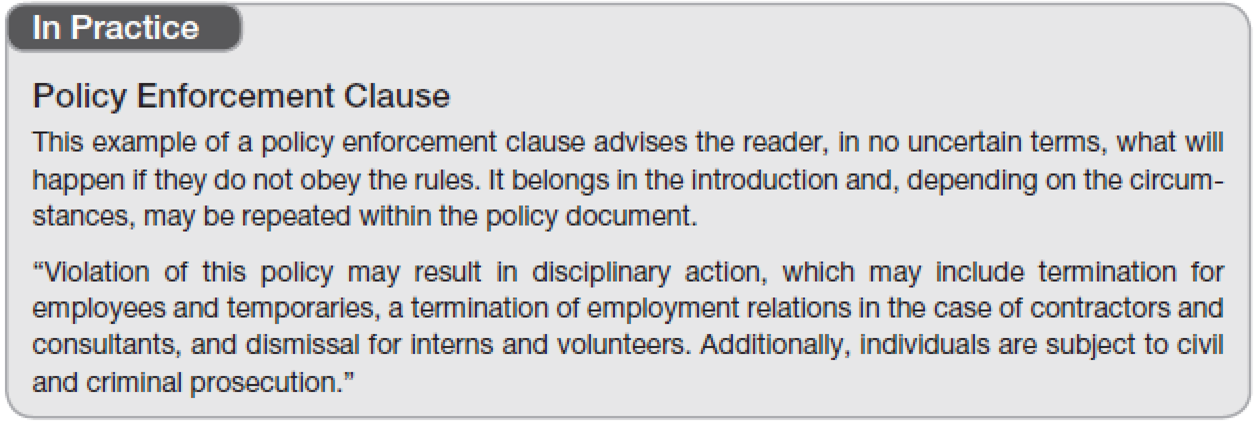
The process for granting post-adoption exemptions should be included in the introduction. Here's an example:

"Where compliance is not technically feasible or as justified by business needs, an exemption may be granted. Exemption requests must be submitted in writing to the COO, including justification and benefits attributed to the exemption. Unless otherwise stated, the COO and the President have the authority to grant waivers."

Policy Format

Policy Enforcemet Clause

- The best way to deliver the message that policies are mandatory is to include the penalty for violating the rules. The policy enforcement clause is where the sanctions for non-adherence to the policy are unequivocally stated in order to reinforce the seriousness of compliance.
- Obviously, you must be careful with the nature of the penalty. It should be proportional to the rule that was broken, whether it was accidental or intentional and the level of risk the company incurred.
- An effective method of motivating compliance is proactive training. All employees should be trained in the acceptable practices presented in the security policy. Without training, it is hard to fault employees for not knowing they were supposed to act in a certain fashion. Imposing disciplinary actions in such situations can adversely affect morale.



In Practice

Policy Enforcement Clause

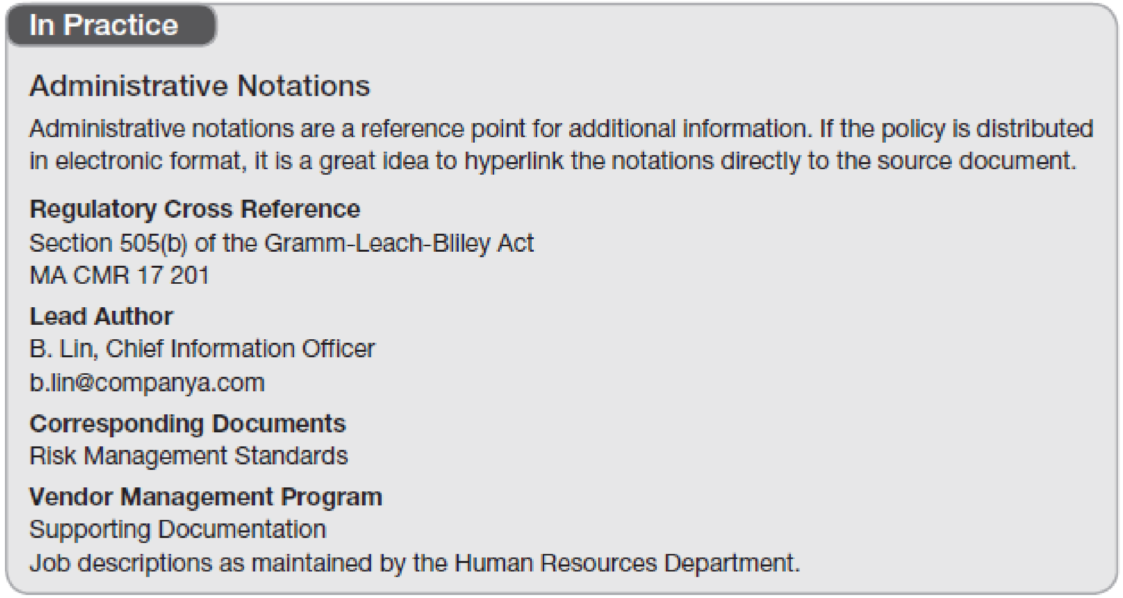
This example of a policy enforcement clause advises the reader, in no uncertain terms, what will happen if they do not obey the rules. It belongs in the introduction and, depending on the circumstances, may be repeated within the policy document.

"Violation of this policy may result in disciplinary action, which may include termination for employees and temporaries, a termination of employment relations in the case of contractors and consultants, and dismissal for interns and volunteers. Additionally, individuals are subject to civil and criminal prosecution."

Policy Format

Administrative Notations

- The purpose of ***administrative notations*** is to refer the reader to additional information and/or provide a reference to an internal resource. Notations include regulatory cross-references, the name of corresponding documents such as standards, guidelines, and programs, supporting documentation such as annual reports or job descriptions, and the policy author’s name and contact information. You should only include notations that are applicable to your organization. However, you should be consistent across all policies.
  - Singular policies incorporate administrative notations either in the heading, at the end of the document, or split between the two locations. How this is handled depends on the policy template used by the company.
  - In a consolidated policy document, the administrative notations are located at the end of each section.



In Practice

Administrative Notations

Administrative notations are a reference point for additional information. If the policy is distributed in electronic format, it is a great idea to hyperlink the notations directly to the source document.

Regulatory Cross Reference
Section 505(b) of the Gramm-Leach-Bliley Act
MA CMR 17 201

Lead Author
B. Lin, Chief Information Officer
b.lin@companya.com

Corresponding Documents
Risk Management Standards

Vendor Management Program
Supporting Documentation
Job descriptions as maintained by the Human Resources Department.

Policy Format

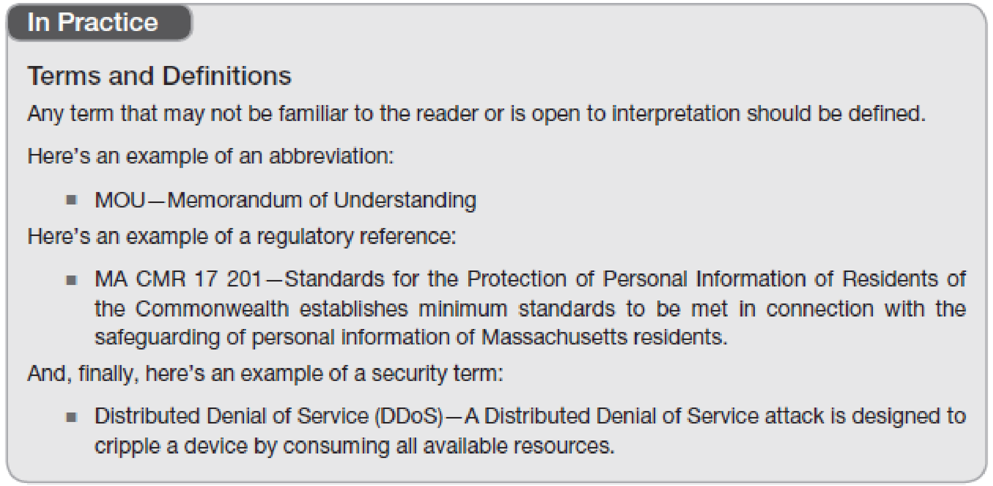
Policy Definitions

- ***The Policy Definition section*** is a glossary of terms, abbreviations, and acronyms used in the document that the reader may be unfamiliar with. Adding definitions to the overall document will aid the target audience in understanding the policy, and will therefore make the policy a much more effective document.
- The rule of thumb is to include definitions for any instance of industry-specific, technical, legal, or regulatory language. When deciding what terms to include, it makes sense to err on the side of caution. The purpose of the security policy as a document is communication and education. The target audience for this document usually encompasses all employees of the company, and sometimes outside personnel.
- Even if some technical topics are well known to all in-house employees, some of those outside individuals who come in contact with the company—and therefore are governed by the security policy - may not be as well versed in the policy’s technical aspects.

Policy Format

Policy Definitions

- Simply put, before you begin writing down definitions, it is recommended to first define the target audience for whom the document is crafted, and cater to the lowest common denominator to ensure optimum communication efficiency.
- Another reason why definitions should not be ignored is for the legal ramification they represent. An employee cannot pretend to have thought that a certain term used in the policy meant one thing when it is clearly defined in the policy itself. When you’re choosing which words will be defined, therefore, it is important not only to look at those that could clearly be unknown, but also those that should be defined to remove any and all ambiguity. A security policy could be an instrumental part of legal proceedings and should therefore be viewed as a legal document and crafted as such.



In Practice

Terms and Definitions

Any term that may not be familiar to the reader or is open to interpretation should be defined.

Here’s an example of an abbreviation:

- MOU—Memorandum of Understanding

Here’s an example of a regulatory reference:

- MA CMR 17 201—Standards for the Protection of Personal Information of Residents of the Commonwealth establishes minimum standards to be met in connection with the safeguarding of personal information of Massachusetts residents.

And, finally, here’s an example of a security term:

- Distributed Denial of Service (DDoS)—A Distributed Denial of Service attack is designed to cripple a device by consuming all available resources.

Writing Style and Technique

- Style is critical. The first impression of a document is based on its style and organization. If the reader is immediately intimated, the contents become irrelevant. Keep in mind that the role of policy is to guide behavior. That can only happen if the roadmap is clear and easy to use.
- How the document flows and the words you use will make all the difference as to how the policy is interpreted. Know your intended reader and write in a way that is understandable. Use terminology that is relevant. Most importantly, keep it simple. Polices that are overly complex tend to be misinterpreted. Policies should be written using plain language.

Using Plain Language

- The term plain language means using the simplest, most straightforward way to express an idea. No one technique defines plain language. Rather, plain language is defined by results—it is easy to read, understand, and use. Studies have proven that documents created using plain-language techniques are effective in a number of ways:
  - Readers understand documents better.
  - Readers prefer plain language.
  - Readers locate information faster.
  - Documents are easier to update.
  - It is easier to train people.
  - Plain language saves time and money.

Writing Style and Technique

Plain Language Techniques for Policy Writing

- The Plain Language Action and Information Network (PLAIN) describes itself on its website (http://plainlanguage.gov) as a group of federal employees from many different agencies and specialties, who support the use of clear communication in government writing. In March of 2011, PLAIN published the Federal Plain Language Guidelines. Some of the guidelines are specific to government publications.
- Many are applicable to both government and industry. The ten guidelines, listed here, are pertinent to writing policies and companion documents:

  1. Write for your audience. Use language your audience knows and is familiar with.
  2. Write short sentences. Express only one idea in each sentence.
  3. Limit a paragraph to one subject. Aim for no more than seven lines.
  4. Be concise. Leave out unnecessary words. Instead of, “for the purpose of,” use “to.” Instead of, “due to the fact,” use “because.”
  5. Don’t use jargon or technical terms when everyday words have the same meaning.
  6. Use active voice. A sentence written in the active voice shows the subject acting in standard English sentence order: subject-verb-object. Active voice makes it clear who is supposed to do what. It eliminates ambiguity about responsibilities. Not “It must be done” but “You must do it.”

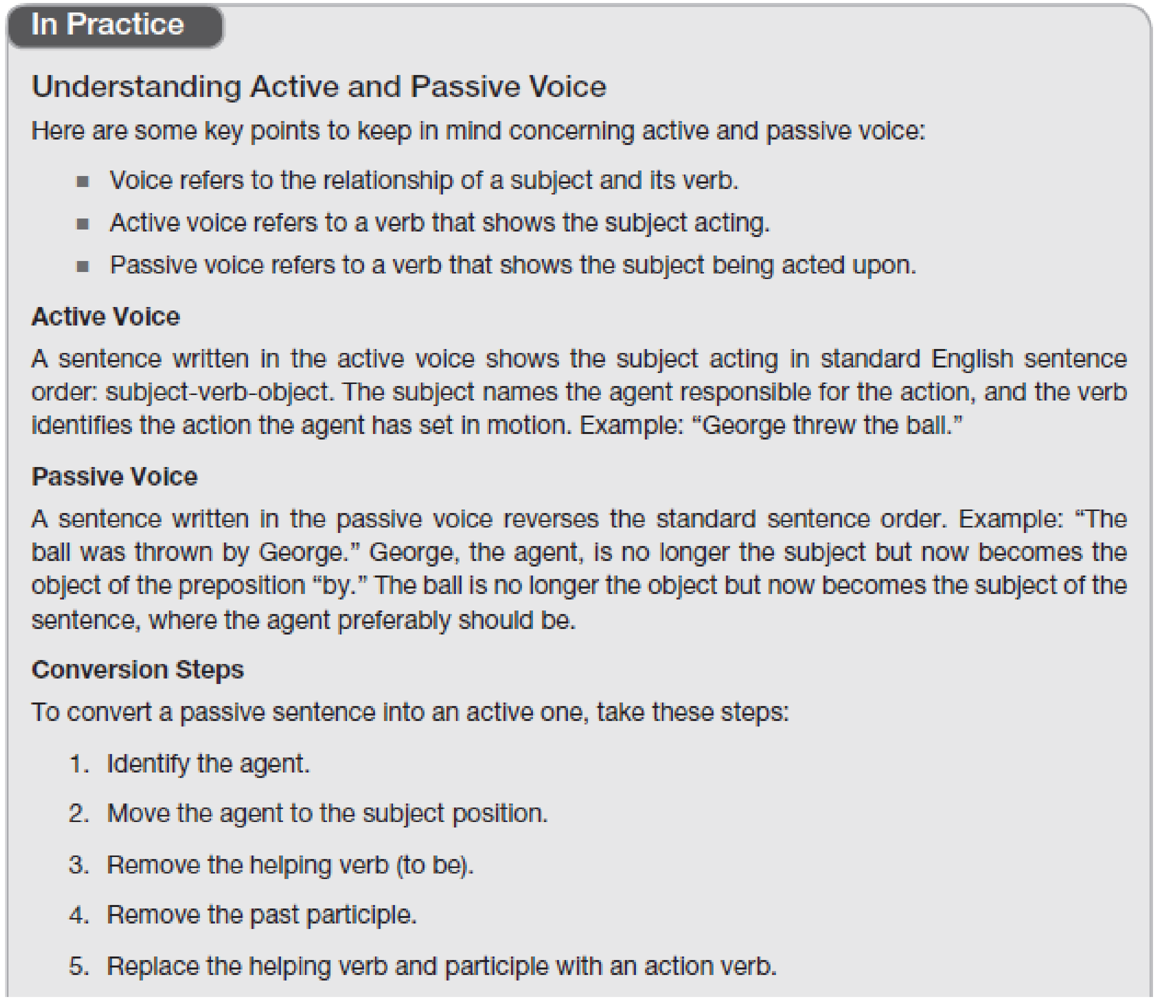
Writing Style and Technique

Plain Language Techniques for Policy Writing

7. Use “must” not “shall” to indicate requirements. “Shall” is imprecise. It can indicate either an obligation or a prediction. The word “must” is the clearest way to convey to your audience that they have to do something.
8. Use words and terms consistently throughout your documents. If you use the term “senior citizens” to refer to a group, continue to use this term throughout your document. Don’t substitute another term, such as “the elderly” or “the aged.” Using a different term may cause the reader to wonder if you are referring to the same group.
9. Omit redundant pairs or modifiers. For example, instead of “cease and desist,” use either “cease” or “desist.” Even better, use a simpler word such as “stop.” Instead of saying “the end result was the honest truth,” say “the result was the truth.”
10. Avoid double negatives and exceptions to exceptions. Many ordinary words have a negative meaning, such as unless, fail to, notwithstanding, except, other than, unlawful (“un-” words), disallowed (“dis-” words), terminate, void, insufficient, and so on. Watch out for them when they appear after “not.” Find a positive word to express your meaning.

Writing Style and Technique

Plain Language Techniques for Policy Writing



In Practice

Understanding Active and Passive Voice

Here are some key points to keep in mind concerning active and passive voice:

- Voice refers to the relationship of a subject and its verb.
- Active voice refers to a verb that shows the subject acting.
- Passive voice refers to a verb that shows the subject being acted upon.

Active Voice

A sentence written in the active voice shows the subject acting in standard English sentence order: subject-verb-object. The subject names the agent responsible for the action, and the verb identifies the action the agent has set in motion. Example: “George threw the ball.”

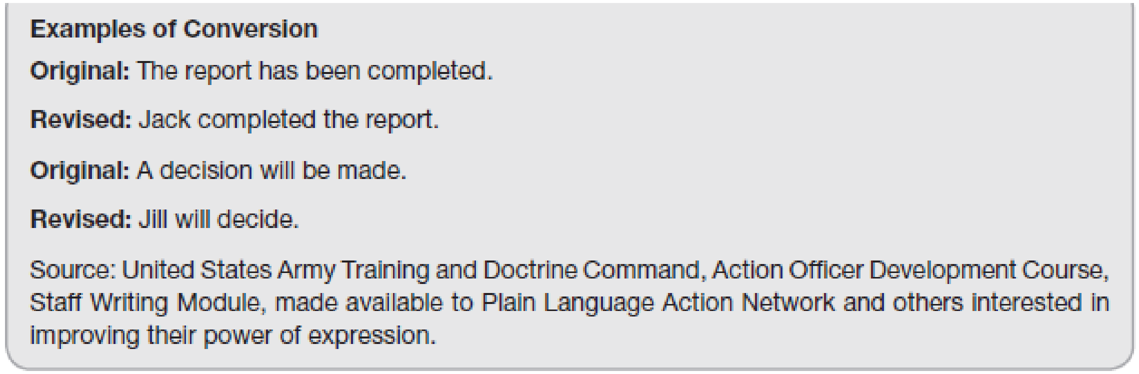
Passive Voice

A sentence written in the passive voice reverses the standard sentence order. Example: “The ball was thrown by George.” George, the agent, is no longer the subject but now becomes the object of the preposition “by.” The ball is no longer the object but now becomes the subject of the sentence, where the agent preferably should be.

Conversion Steps

To convert a passive sentence into an active one, take these steps:

1. Identify the agent.
2. Move the agent to the subject position.
3. Remove the helping verb (to be).
4. Remove the past participle.
5. Replace the helping verb and participle with an action verb.



Examples of Conversion

Original: The report has been completed.

Revised: Jack completed the report.

Original: A decision will be made.

Revised: Jill will decide.

Source: United States Army Training and Doctrine Command, Action Officer Development Course, Staff Writing Module, made available to Plain Language Action Network and others interested in improving their power of expression.

Thank You

MyUTeM

www.utem.edu.my

Key Policies Every Organization Needs

- Information Classification Security Policy
- Acceptable Use Policy
- Minimum Access Policy
- Network Access Policy
- Remote Access
- Acceptable Encryption Policy
- Web Server Security Policy
- Extranet Policy
- Application Service Provider Policy
- Authentication Credentials Policy

(You find examples of many of these policies (and more) on the SANS Policy website at:
http://www.sans.org/resources/policies/)

Other Potential Policies

- Application Container Policy
- Database Credential Coding Policy
- Database Execution Environment Policy
- Highly Sensitive Application Server Policy
- Inter-process Communication Policy
- Internet DMZ Equipment Policy
- DMZ Application Server Policy
- Internet DMZ Web Entitlement Policy
- DMZ Lab Security Policy
- Account Access Request Policy
- Acquisition Assessment Policy
- Audit Policy
- Risk Assessment Policy
- Router and Switch Security Policy
- Server Security Policy
- Wireless Policy
- Lab Anti-virus Policy
- Internal Lab Security Policy
- Email Security Policy

(You find examples of many of these policies (and more) on the SANS Policy website at:

http://www.sans.org/resources/policies/)

Policy Resources

- The SANS Policy Website
  - https://www.sans.org/security-resources/policies/
- EDUCAUSE Information security policy examples
  - https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/security-policies/information-security-policy-examples