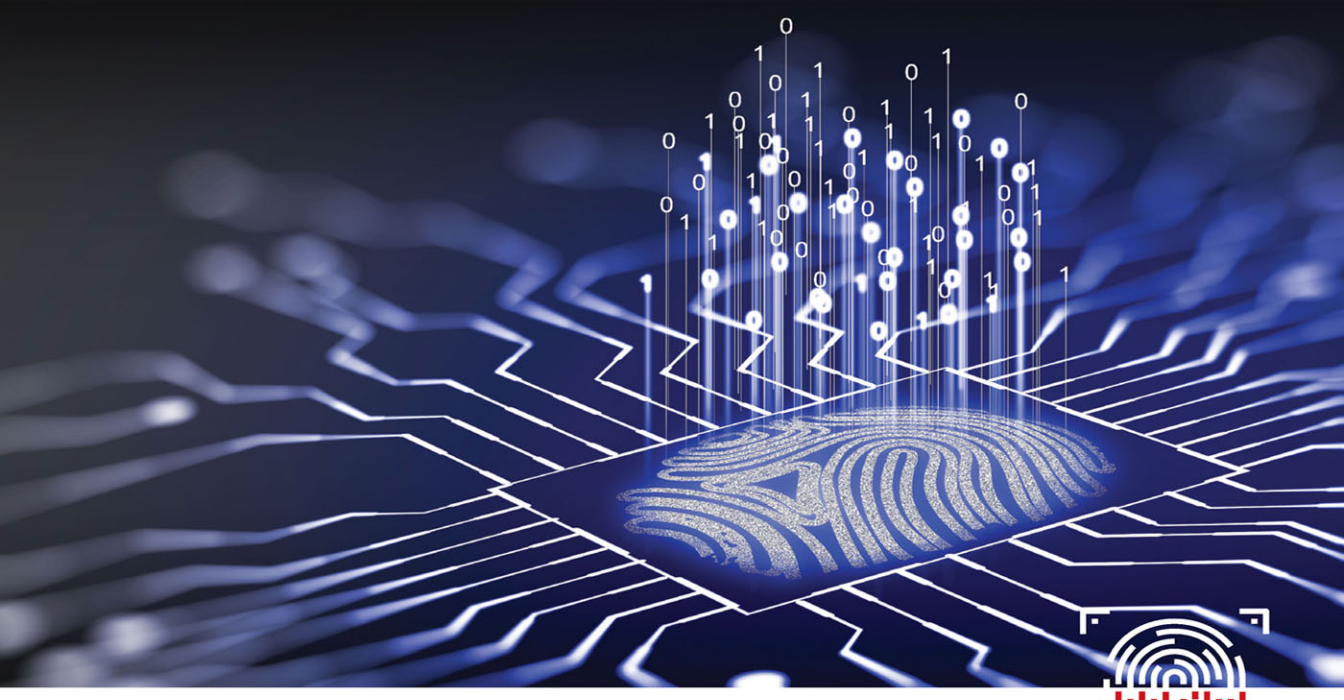

FOURTH EDITION

DEVELOPING CYBERSECURITY PROGRAMS AND POLICIES IN AN AI-DRIVEN WORLD

OMAR SANTOS

FREE SAMPLE CHAPTER |

Developing Cybersecurity Programs and Policies in an AI-Driven World

Fourth Edition

Omar Santos

PEARSON

Hoboken, New Jersey

Developing Cybersecurity Programs and Policies in an AI-Driven World

Fourth Edition

ISBN-13: 978-0-13-807410-4
ISBN-10: 0-13-807410-0

Library of Congress Cataloging-in-Publication Data: 2024909456

$PrintCode

GM K12, Early Career and Professional Learning
Soo Kang

Director, ITP Product Management
Brett Bartow

Executive Editor
James Manly

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Timothy Wright

Proofreader
Donna E. Mulder

Technical Editor
John Stuppi

Publishing Coordinator
Cindy Teeters

Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

Table of Contents

About the Author

Omar Santos is a Distinguished Engineer at Cisco, focusing on artificial intelligence (AI) security, cybersecurity research, incident response, and vulnerability disclosure. He is a board member of the OASIS Open standards organization and the founder of OpenEoX. Omar's collaborative efforts extend to numerous organizations, including the Forum of Incident Response and Security Teams (FIRST) and the Industry Consortium for Advancement of Security on the Internet (ICASI). Omar is the co-chair of the FIRST PSIRT Special Interest Group (SIG). Omar is the co-founder of the DEF CON Red Team Village and the chair of the Common Security Advisory Framework (CSAF) technical committee.

Omar is the author of more than 25 books, 21 video courses, and more than 50 academic research papers. He is a renowned expert in ethical hacking, vulnerability research, incident response, and AI security. He employs his deep understanding of these disciplines to help organizations stay ahead of emerging threats. His dedication to cybersecurity has made a significant impact on technology standards, businesses, academic institutions, government agencies, and other entities striving to improve their cybersecurity programs. Prior to working for Cisco, Omar served in the U.S. Marines, focusing on the deployment, testing, and maintenance of Command, Control, Communications, Computer and Intelligence (C4I) systems. **You can find Omar at:**

X: @santosomar

LinkedIn: https://www.linkedin.com/in/santosomar

Dedication

I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.
I also dedicate this book to the memory of my father, Jose, and my mother, Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

Acknowledgments

This book is a result of concerted efforts of various individuals. Without their help, this book would have not become a reality. I would like to thank the technical reviewer and my friend, John Stuppi, for his contributions and expert guidance.

I would also like to express my gratitude to Chris Cleveland, development editor, and James Manly, executive editor, for their help and continuous support during the development of this book.

About the Technical Reviewer

John Stuppi, CCIE No. 11154, is an Engineering Program Manager in the Security & Trust Organization (S&TO) at Cisco where he works with Cisco customers to investigate suspected compromises in their network environment and to protect their networks against existing and emerging cybersecurity threats, risks, and vulnerabilities. Current projects include working with newly acquired entities to integrate them into Cisco's PSIRT Vulnerability Management processes and advising some of Cisco's most strategic customers on vulnerability management and risk assessment. John has presented multiple times on various network security topics at Cisco Live, Black Hat, as well as other customer-facing cybersecurity conferences. John is also the co-author of the *Official Certification Guide for CCNA Security 210-260* published by Cisco Press. Additionally, John has contributed to the Cisco Security Portal through the publication of white papers, Security Blog posts, and Cyber Risk Report articles. Prior to joining Cisco, John worked as a network engineer for JPMorgan and then as a network security engineer at Time, Inc., with both positions based in New York City. John is also a CISSP (#25525) and holds AWS Cloud Practitioner and Information Systems Security (INFOSEC) Professional Certifications. In addition, John has a BSEE from Lehigh University and an MBA from Rutgers University. John splits his time between Eatontown, New Jersey, and Clemson, South Carolina, with his wife, son, and daughter.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *Developing Cybersecurity Programs and Policies in an AI-Driven World* for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780138074104 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

The number of cyber attacks continues to rise. Demand for safe and secure data and other concerns mean that companies need professionals to keep their information safe. Cybersecurity risk includes not only the risk of a data breach but the risk of an entire organization being undermined via business activities that rely on digitization and accessibility. As a result, learning how to develop an adequate cybersecurity program is crucial for any organization. Cybersecurity can no longer be something that you delegate to the information technology (IT) team. Everyone needs to be involved, including the board of directors.

This book focuses on industry-leading practices and standards, such as the International Organization for Standardization (ISO) standards and the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Special Publications. This book is meticulously crafted for cybersecurity professionals, policymakers, and organizational leaders aiming to fortify their defenses in a world increasingly dominated by sophisticated threats, including emerging technologies such as artificial intelligence (AI).

This book begins with a foundational overview of cybersecurity policy and governance to set the stage for the need for balance between policy and practicality in cybersecurity programs. It then goes into detail on cybersecurity policy organization, format, and styles, providing insights into crafting effective and adaptable policies.

As the book progresses, it covers topics such as cloud security, governance and risk management, and asset management and data loss prevention, which are just some of the multifaceted challenges organizations face in securing their assets. Cloud security is paramount in today's environments because of the need to protect data, applications, and infrastructures operated over the cloud. As businesses and organizations increasingly use cloud services, the complexity and volume of cyber threats escalate. Cloud security is important to ensure compliance with rigorous regulatory requirements and industry standards. It plays a crucial role in enabling the safe adoption of cloud technologies, enabling innovation and agility.

The book also addresses the human element in a chapter on human resources security and education, recognizing that technology alone cannot safeguard against threats without informed and well-equipped personnel. The book also has chapters dedicated to cybersecurity operations, access control management, and supply chain security, highlighting the critical role of advanced technologies in detecting, mitigating, and responding to threats. A chapter on business continuity management emphasizes the importance of resilience and preparedness in the face of disruptions.

Given the complexity of today's regulatory landscape, this book provides great guidance on compliance across many sectors, including financial institutions, health care, technology, and retail. The last two chapters, which focus on privacy in an AI-driven landscape and AI governance and regulations, offer a forward-looking perspective on the ethical, legal, and societal implications of today's fast-paced world.

We used to say that we "stand on the brink of a new era." Well, that new era has arrived. The integration of AI into cybersecurity practices is no longer a futuristic vision but today's reality. The discussions in the last two chapters of this book are crucial for developing robust frameworks that protect against sophisticated threats and also ensure the responsible use of emerging technologies. I hope you find this book to be a roadmap for navigating the complexities of cybersecurity in the age of AI—and not just another cybersecurity book. I hope that it will equip you with the knowledge, strategies, and insights needed to create dynamic and resilient cybersecurity programs and policies.

Credits

Figure 15.1 & 15.2 - Gegear/Shutterstock

Figure 11.3 - X Corp.

Figure 14.9 - United States department of Health and Human Services

Figure 17.5 - People and AI Research

Chapter 2

Cybersecurity Policy Organization, Format, and Styles

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Explain the differences between a policy, a standard, a procedure, a guideline, and a plan.
- Know how to use plain language when creating and updating your cybersecurity policy.
- Identify the different policy elements.
- Include the proper information in each element of a policy.

In Chapter 1, "Understanding Cybersecurity Policy and Governance," you learned that policies have played a significant role in helping us form and sustain our social, government, and corporate organizations. In this chapter, we begin by examining the hierarchy and purpose of guiding principles, policy, standards, procedures, and guidelines, as well as adjunct plans and programs. Returning to our focus on policies, we examine the standard components and composition of a policy document. You will learn that even a well-constructed policy is useless if it doesn't deliver the intended message. The end result of complex, ambiguous, or bloated policy is, at best, noncompliance. At worst, negative consequences result as such policies may not be followed or understood. In this chapter, you will be introduced to "plain language," which involves using the simplest, most straightforward way to express an idea. Plain-language documents are easy to read, understand, and act on. By the end of the chapter, you will have the skills to construct policy and companion documents. This chapter focuses on cybersecurity policies in the private sector and not policies created by governments of any country or state.

Policy Hierarchy

As you learned in Chapter 1, 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 a governance objective. The relationship between the documents is known as the ***policy hierarchy***. In a hierarchy, with the exception of the topmost object, each object is subordinate to the one above it. In a policy hierarchy, the topmost objective is the guiding principles, as illustrated in Figure 2-1.

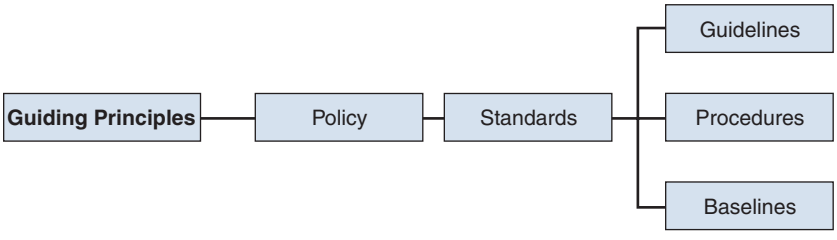

FIGURE 2-1 Policy Hierarchy

Cybersecurity policies should reflect the guiding principles and organizational objectives. This is why it is very important to communicate clear and well-understood organizational objectives within an organization. Standards are a set of rules and mandatory actions that provide support to a policy. Guidelines, procedures, and baselines provide support to standards. Let's take a closer look at each of these concepts.

Standards

Standards serve as specifications for the implementation of policy and dictate mandatory requirements. For example, you might have a remote worker policy that states the following:

- This policy ensures that all employees understand their obligations to maintain a secure, productive, and efficient work environment while working from a remote location.
- This policy applies to all employees who are approved to work remotely, either on a full-time, part-time, or temporary basis.
- Employees must be reachable via phone, email, or video conferencing during core work hours.
- Company-issued equipment should be used for work purposes only and should be maintained in a secure manner.
- Employees must adhere to the organization's data security policy, including but not limited to, use of the VPN, use of approved cloud services, secure data transfer, and storage solutions.

The remote worker standard would then dictate the required characteristics, such as the following:

- MFA must be enabled for all accounts accessing corporate resources.
- All devices used for remote work must have up-to-date anti-malware software installed.
- Laptops and workstations used for remote work must have full-disk encryption enabled.
- No sensitive data should be stored locally unless approved and encrypted. Use corporate cloud storage solutions when possible.
- Only software approved by the IT department may be installed on work devices.
- Keep all operating systems and applications updated with the latest security patches.
- Remote devices and activity may be audited periodically for compliance with this standard.
- Failure to adhere to this standard may result in disciplinary actions, as described in the Remote Work Policy.

Another example of a standard is a common configuration of infrastructure devices such as routers and switches. An organization may have dozens, hundreds, or even thousands of routers and switches, and it might have a "standard" way of configuring authentication, authorization, and accounting (AAA) for administrative sessions. It might use TACACS+ or RADIUS as the authentication standard mechanism for all routers and switches within the organization.

As you can see, a policy represents expectations that are not necessarily subject to changes in technology, processes, or management. A standard, on the other hand, is very specific to the infrastructure.

Standards are determined by management, and unlike policies, they are not subject to authorization by the board of directors. Standards can be changed by management as long as they conform to the intent of the policy. A difficult task of writing a successful standard for a cybersecurity program is achieving consensus by all stakeholders and teams within an organization. In addition, a standard does not have to address everything that is defined in a policy. Standards should be compulsory and must be enforced to be effective.

Baselines

A ***baseline*** serves as a standard guideline or set of specifications that is applicable to a particular category or group within an organization. These groups can be defined by different factors such as the platform (including specific operating systems and their versions), device type (like laptops, servers, desktops, routers, switches, firewalls, and mobile devices), ownership status (whether devices are employee-owned or corporate-owned), and location (such as onsite or remote workers).

The main purpose of establishing baselines is to ensure uniformity and consistency across the organization's technological environment. For instance, in the context of a policy for remote workers, a baseline might require that all Windows devices used by remote employees adhere to a specific Active Directory Group Policy configuration. This standard configuration is used to technically enforce security requirements, ensuring that all devices within this group meet a consistent level of security compliance. This approach helps in managing and securing IT resources effectively, particularly in diverse and distributed environments.

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 remote worker standard in the previous example might read like this:

- Use MFA all the time. MFA is a security measure that requires you to provide two or more forms of identification before you can access your account. This usually means entering your password (something you know) plus a second form of identification—like a code sent to your phone (something you have) or a face recognition scan (something you are).
- Store your device in a secure place when it is not in use to minimize the risk of theft or unauthorized access.
- Regularly back up important files to the corporate cloud storage solution, not to personal cloud or local storage.
- Use secure methods to delete sensitive information from your device rather than just moving files to the recycle bin.

Guidelines are recommendations and advice to users when certain standards do not apply to the environment. Guidelines are designed to streamline certain processes according to best practices and must be consistent with the cybersecurity policies. At the same time, guidelines often are open to interpretation and do not need to be followed to the letter.

Procedures

Procedures are instructions for how a policy, a standard, a baseline, and guidelines are carried out in a given situation. Procedures focus on actions or steps, with specific starting and ending points. 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:** Uses either pictures or symbols to illustrate the step.
- **Flowchart:** Used when a decision-making process is associated with the task. Flowcharts are useful when multiple parties are involved in separate tasks.

> **Note**
>
> As with guidelines, when designing procedures, it is important to know both your audience and the complexity of the task. In Chapter 9, "Cybersecurity Operations (CyberOps), Incident Response, Digital Forensics, and Threat Hunting," we discuss in detail the use of incident response playbooks and other standard operating procedures (SOPs).

Procedures should be well documented and easy to follow to ensure consistency and adherence to policies, standards, and baselines. Like policies and standards, they should be well reviewed to ensure that they accomplish the objective of the policy and that they are accurate and remain relevant.

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 time frame, 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 we discuss in this book:

- Vendor management plan
- Incident response plan
- Business continuity plan
- Disaster recovery plan

Policies and plans are closely related. For example, an incident response policy generally includes 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.

In Practice

Policy Hierarchy Review

Let's look at an example of how standards, guidelines, and procedures support a policy statement:

- The policy requires that all media should be encrypted.
- The standard specifies the type of encryption that must be used.
- The guideline illustrates how to identify removable media.
- The procedure provides instructions for encrypting the media.

Writing Style and Technique

Style is critical. A reader's first impression of a document is based on its style and organization. If the reader is immediately intimidated, the contents become irrelevant. Keep in mind that the role of policy is to guide behavior. That can happen only if the policy is clear and easy to use. How the document flows and the words you use will make all the difference in 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. Policies 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 single 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:[1]

- 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.

Even confident readers appreciate plain language. It enables them to read more quickly and with increased comprehension. The use of plain language is spreading in many areas of American culture, including governments at all levels, especially the federal government, health care, the sciences, and the legal system.

FYI: Warren Buffet on Using Plain Language

The following excerpt from the preface to the Securities and Exchange Commission's *A Plain English Handbook* was written by Berkshire Hathaway co-founder, chair, and CEO Warren Buffett:

> For more than forty years, I've studied the documents that public companies file. Too often, I've been unable to decipher just what is being said or, worse yet, had to conclude that nothing was being said.
>
> Perhaps the most common problem, however, is that a well-intentioned and informed writer simply fails to get the message across to an intelligent, interested reader. In that case, stilted jargon and complex constructions are usually the villains.
>
> One unoriginal but useful tip: Write with a specific person in mind. When writing Berkshire Hathaway's annual report, I pretend that I'm talking to my sisters. I have no trouble picturing them: Though highly intelligent, they are not experts in accounting or finance. They will understand plain English, but jargon may puzzle them. My goal is simply to give them the information I would wish them to supply me if our positions were reversed. To succeed, I don't need to be Shakespeare; I must, though, have a sincere desire to inform.
>
> No siblings to write to? Borrow mine: Just begin with "Dear Doris and Bertie."

Source: Securities and Exchange Commission, "A Plain English Handbook: How to Create Clear SEC Disclosure Documents," https://www.sec.gov/pdf/handbook.pdf.

The Plain Language Movement

It seems obvious that everyone would want to use plain language, but as it turns out, that is not the case. There is an enduring myth that to appear official or important, documents should be verbose. The result has been a plethora of complex and confusing regulations, contracts, and, yes, policies. In response to public frustration, the plain language movement began in earnest in the early 1970s.

In 1971, the National Council of Teachers of English in the United States formed the Public Doublespeak Committee. In 1972, U.S. President Richard Nixon created plain language momentum when he decreed that the "Federal Register be written in 'layman's terms.'" The next major event in the U.S. history of plain language occurred in 1978, when U.S. President Jimmy Carter issued Executive Orders 12044 and 12174, with the goal of making government regulations cost-effective and easy to understand. In 1981, U.S. President Ronald Reagan rescinded Carter's executive orders. Nevertheless, many continued their efforts to simplify documents; by 1991, eight states had passed statutes related to plain language.

In 1998, President Clinton issued a Presidential Memorandum requiring government agencies to use plain language in communications with the public. All subsequent administrations have supported this memorandum. In 2010, plain-language advocates achieved a major victory when the Plain Writing Act was passed. This law requires federal government agencies to write publications and forms in a "clear, concise, well-organized" manner, following plain language guidelines.

We can take a cue from the government and apply these same techniques when writing policies, standards, guidelines, and plans. The easier a policy is to understand, the better the chance of compliance.

FYI: Plain Language Results

This is an example of using plain language provided by the U.S. government.

Before

Infants and children who drink water containing lead in excess of the action level could experience delays in their physical or mental development. Children could show slight deficits in attention span and learning abilities. Adults who drink this water over many years could develop kidney problems or high blood pressure.

After

Lead in drinking water can make you sick. Here are some possible health effects of high lead levels in your drinking water:

Children:

- Delayed growth
- Learning disabilities
- Short attention span

Adults:

- Kidney problems
- High blood pressure

Source: Plain Language Action and Information Network (PLAIN), "Lead in Water" example, https://www.plainlanguage.gov/examples/before-and-after/lead-warning.

Plain Language Techniques for Policy Writing

The Plain Language Action and Information Network (PLAIN) describes itself on its website (https://plainlanguage.gov) as a group of federal employees from many agencies and specialties who support the use of clear communication in government writing. In March 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 10 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 that," use "because."
5. Don't use jargon or technical terms when you can use everyday words that have the same meaning.
6. Use active voice. A sentence written in 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."
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 terms 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.

Want to learn more about using plain language? The official website of PLAIN has a wealth of resources, including the Federal Plain Language Guidelines, training materials and presentations, videos, posters, and references.

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 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 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: Stefan completed the report.

Original: A decision will be made.

Revised: Derek will decide.

In Practice

U.S. Army Clarity Index

The Clarity Index was developed to encourage plain writing. The index has two factors: average number of words per sentence and percentage of words longer than three syllables. The index adds together the two factors. The target is an average of 15 words per sentence and 15% of the total text being composed of three syllables or less. A resulting index between 20 and 40 is ideal and indicates the right balance of words and sentence length. In the following example (excerpted from Warren Buffet’s SEC introduction), the index is composed of an average of 18.5 words per sentence, and 11.5% of the words are three syllables or less. At an index of 30, this text falls squarely in the ideal range!

Sentence	Number of Words per Sentence	Number and Percentage of Words with Three or More Syllables
For more than forty years, I've studied the documents that public companies file.	13	Two words: 2/13 = 15%
Too often, I've been unable to decipher just what is being said or, worse yet, had to conclude that nothing was being said.	23	One word: 1/23 = 4%
Perhaps the most common problem, however, is that a well-intentioned and informed writer simply fails to get the message across to an intelligent, interested reader.	26	Three words: 3/26 = 11%
In that case, stilted jargon and complex constructions are usually the villains.	12	Two words: 2/12 = 16%
Total	74	46%
Average	18.5	11.5%
Clarity Index	**18.5 + 11.5 = 30**	

Policy Format

Writing policy documents can be challenging. Policies are complex documents that must be written to withstand legal and regulatory scrutiny and at the same time must be easy for a reader to read and understand. The starting point for choosing a format is identifying the policy audience.

Understand Your Audience

Who a 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. For example, 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 chief information security officer (CISO). The policy, or portions of it, can sometimes apply to people outside the company, such as business partners, service providers, contractors, or consultants. The policy audience is a potential resource during the entire policy life cycle. 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 Types

Organize before you begin writing! It is important to decide how many sections and subsections you will require before you begin writing. Designing a template that allows the flexibility of editing will save considerable time and reduce aggravation. In this section, you will learn about the different sections and subsections of a policy, as well as the policy document formation options.

There are two general ways to structure and format a policy:

- **Singular policy:** Write each policy as a discrete document.
- **Consolidated policy:** Group together similar and related policies.

Consolidated policies are often organized by section and subsection.

Table 2-1 illustrates policy document format options.

TABLE 2-1 Policy Document Format Options

Format	Example
Singular policy	Chief information security officer (CISO) policy: Specific to the role and responsibility of the information security officer.
Consolidated policy	Governance policy: Addresses the role and responsibilities of the board of directors, executive management, chief risk officer, CISO, compliance officer, legal counsel, auditor, IT director, and users.

The advantage of creating individual policies is that each policy document can be short, clean, 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 of a consolidated policy is that it presents a composite management statement in a single voice. The disadvantages are the potential size of the document and the difficulty the reader may have locating applicable sections.

In the first edition of this book, we limited our study to singular policy documents. Since then, both the use of technology and the regulatory landscape have increased exponentially—only outpaced by escalating threats. In response to this ever-changing environment, the need for policies and the number of policies has grown. For many organizations, managing singular policies has become unwieldy. The current trend is toward consolidation. Throughout this edition, we have consolidated policies by security domain.

Regardless of which format you choose, you should not include standards, baselines, guidelines, or procedures in your policy document. If you do, you will end up with one big unruly document. And 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 it. This will become very costly and cumbersome for everyone involved.

Policy Components

Policy documents have multiple sections or components (see Table 2-2). How the components are used and in what order depends on which format—singular or consolidated—you choose. In this section, we examine the composition of each component. Consolidated policy examples are provided in the "In Practice" sidebars.

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

Version Control

Best practices dictate that policies are reviewed annually to ensure that 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. The version is 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, the 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 a singular policy document, this information is split between the policy heading and the administrative notation sections.
- For a consolidated policy document, a version control table is included either at the beginning of the document or at the beginning of a section.

In Practice

Version Control Table

A consolidated policy document includes a version control table. 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	2024-07-17
1.1	S. Ford, EVP	Subsection addition	2.5: Disclosures to Third Parties.	Sr. management committee	2024-08-14
1.2	S. Ford, EVP	Subsection update	4.4: Border Device Management 5.8: Wireless Networks	Sr. management committee	2025-02-25
—	S. Ford, EVP	Annual review	No change	Sr. management committee	2025-07-18
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	2025-09-19

Introduction

Think of the introduction as the opening act. This is where authors first meet the readers 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 and adhering to the policy
- To acquaint the reader with the document and its contents
- To explain the exemption process as well as the consequence of noncompliance
- To reinforce the authority of the policy

The first part of the introduction should make the case for why the policy is 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 chair of the board, CEO, or president, is appropriate. Users should understand that they are unequivocally and directly responsible for following the policy in the course of their normal employment or relationship with the company. This part of the introduction should also make clear that questions are welcome, and a resource is available who can clarify the policy and/or assist with compliance.

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. In some cases, the introduction includes a revision history, the stakeholders who may have reviewed the policy, and who to contact to make any modifications.

The fourth part of the introduction should explain how to handle situations where compliance may not be feasible. It should provide a high-level view of the exemption and enforcement process. The section should also address the consequences of willful noncompliance.

- For a singular policy document, the introduction should be a separate document.
- For a consolidated policy document, the introduction serves as the preface and follows the version control table.

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, finally, 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 Cybersecurity 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 Cybersecurity 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 Cybersecurity Policy is organized by category. These categories form the framework of our Cybersecurity 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.

—Anthony Starks, Chief Executive Officer (CEO)

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:

- A singular policy must be able to stand on its 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.

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 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 be at risk of 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.

- A singular policy lists 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 Statement

Up to this point in the document, we have discussed everything but the actual policy statement. The ***policy statement*** is 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.

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 Cybersecurity 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 Cybersecurity 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 organization's adherence to the Cybersecurity 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 Cybersecurity 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 control 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 Cybersecurity Policy and the Vendor Management Program.

Policy Exceptions and the Exemption Process

Realistically, there will be situations in which 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 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. Only the method or process for requesting an exemption—and not the criteria or conditions for exemptions—should be detailed in the policy. Trying to list all the conditions to which exemptions apply can lead to 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.

Finally, it is recommended that you 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.
- It can become difficult to keep track of and successfully audit a large number of exceptions and exemptions.

If there are too many built-in exceptions and/or exemption requests, it may indicate 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 Enforcement 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 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. We take a look at various training, education, and awareness tools and techniques in later chapters.

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.

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 names 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 include only notations that are applicable to your organization. However, you should be consistent across all policies.

- A singular policy incorporates 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 company's policy template.
- 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@example.com

Corresponding Documents

Risk Management Standards

Vendor Management Program

Supporting Documentation

Job descriptions as maintained by the Human Resources Department

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 general rule 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 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.

Simply put, before you begin writing down definitions, it is recommended that you 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 definitions should not be ignored is for the legal ramifications 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 to look not only at those that could clearly be unknown but also at 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 are a few examples of security terms that might be included:

- **Distributed Denial of Service (DDoS):** An attack in which there is a massive volume of IP packets from multiple sources. The flood of incoming packets consumes available resources, resulting in denial of service to legitimate users.
- **Exploit:** A malicious program designed to exploit, or take advantage of, a single vulnerability or set of vulnerabilities.

- **Phishing:** An attack in which the attacker presents to a user a link that looks like a valid, trusted resource. A user who clicks it is prompted to disclose confidential information such as their username and password.
- **Pharming:** A technique an attacker uses to direct a customer's URL from a valid resource to a malicious one that could be made to appear as the valid site to the user. From there, an attempt is made to extract confidential information from the user.
- **Malvertising:** The act of incorporating malicious ads on trusted websites, which results in users' browsers being inadvertently redirected to sites hosting malware.
- **Logic bomb:** A type of malicious code that is injected into a legitimate application. An attacker can program a logic bomb to delete itself from the disk after it performs the malicious tasks on the system. Examples of these malicious tasks include deleting or corrupting files or databases and executing a specific instruction after certain system conditions are met.
- **Trojan horse:** A type of malware that executes instructions to delete files, steal data, or compromise the integrity of the underlying operating system. Trojan horses typically use a form of social engineering to fool victims into installing such software on their computers or mobile devices. Trojans can also act as backdoors.
- **Backdoor:** A piece of malware or a configuration change that allows an attacker to control the victim's system remotely. For example, a backdoor can open a network port on the affected system so that the attacker can connect and control the system.

Summary

You now know that policies need supporting documents to give them context and meaningful application. Standards, guidelines, and procedures provide a means to communicate specific ways to implement our policies. We create our organizational standards, which specify the requirements for each policy. We offer guidelines to help people comply with standards. We create sets of instructions known as procedures to ensure that tasks are consistently performed. The format of a procedure—simple step, hierarchical, graphic, or flowchart—depends on the complexity of the task and the audience. In addition to creating policies, we create plans or programs to provide strategic and tactical instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain time frame, usually with defined stages and with designated resources.

Writing policy documents is a multistep process. First, we need to define the audience for which the document is intended. Then, we choose the format. Options are to write each policy as a discrete document (singular policy) or to group like policies together (consolidated policy). Finally, we need to decide upon the structure, including the components to include and in what order.

The first and arguably most important section is the introduction. This is our opportunity to connect with the reader and to convey the meaning and importance of our policies. The introduction should be written by the "person in charge," such as the CEO or president. This person should use the introduction to reinforce company-guiding principles and correlate them with the rules introduced in the security policy.

Specific to each policy are the heading, goals and objectives, policy statement, and (if applicable) exceptions. The heading identifies the policy by name and provides the reader with an overview of the policy topic or category. The goals and objectives convey what the policy is intended to accomplish. The policy statement lays out the rules that need to be followed and may reference the implementation instructions (standards) or corresponding programs. Policy exceptions are agreed waivers that are documented within the policy.

An exemption or waiver process is required for exceptions identified after a policy has been authorized. The policy enforcement clause is where the sanctions for willful non-adherence to the policy are unequivocally stated to reinforce the seriousness of compliance. Administrative notations refer the reader to additional information and/or provide references to internal resources. The policy definition section is a glossary of terms, abbreviations, and acronyms used in the document that the reader may be unfamiliar with.

Recognizing that the first impression of a document is based on its style and organization, we studied the work of the plain language movement. Using plain language helps produce documents that are easy to read, understand, and use. We looked at 10 techniques from the Federal Plain Language Guideline that we can (and should) use for writing effective policies. In the next section of the book, we put these newfound skills to use.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. The policy hierarchy is the relationships between which of the following?
   - A. Guiding principles, regulations, laws, and procedures
   - B. Guiding principles, standards, guidelines, and procedures
   - C. Guiding principles, instructions, guidelines, and programs
   - D. None of the above
2. Which of the following statements best describes the purpose of a standard?
   - A. To state the beliefs of an organization
   - B. To reflect the guiding principles
   - C. To dictate mandatory requirements
   - D. To make suggestions
3. Which of the following statements best describes the purpose of a guideline?
   - A. To state the beliefs of an organization
   - B. To reflect the guiding principles
   - C. To dictate mandatory requirements
   - D. To help people conform to a standard
4. Which of the following statements best describes the purpose of a baseline?
   - A. To measure compliance
   - B. To ensure uniformity across a similar set of devices
   - C. To ensure uniformity and consistency
   - D. To make suggestions
5. Simple step, hierarchical, graphic, and flowchart are examples of which of the following formats?
   - A. Policy
   - B. Program
   - C. Procedure
   - D. Standard

6. Which of the following terms best describes instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain time frame, usually with defined stages and with designated resources?

   A. Plan
   B. Policy
   C. Procedure
   D. Package

7. Which of the following statements best describes a disadvantage to using the singular policy format?

   A. The policy can be short.
   B. The policy can be targeted.
   C. You may end up with too many policies to maintain.
   D. The policy can easily be updated.

8. Which of the following statements best describes a disadvantage to using the consolidated policy format?

   A. Consistent language is used throughout the document.
   B. Only one policy document must be maintained.
   C. The format must include a composite management statement.
   D. The document may end up being very long.

9. Policies, standards, guidelines, and procedures should all be in the same document.

   A. True
   B. False
   C. Only if the company is multinational
   D. Only if the documents have the same author

10. Version control is the management of changes to a document and should include which of the following elements?

    A. Version or revision number
    B. Date of authorization or date that the policy took effect
    C. Change description
    D. All of the above

11. What is an exploit?

- **A.** A phishing campaign
- **B.** A malicious program or code designed to exploit, or take advantage of, a single vulnerability or set of vulnerabilities
- **C.** A network or system weakness
- **D.** A protocol weakness

12. The name of the policy, policy number, and overview belong in which of the following sections?

- **A.** Introduction
- **B.** Policy heading
- **C.** Policy goals and objectives
- **D.** Policy statement

13. The aim or intent of a policy is stated in the _____.

- **A.** introduction
- **B.** policy heading
- **C.** policy goals and objectives
- **D.** policy statement

14. Which of the following statements is true?

- **A.** A security policy should include only one objective.
- **B.** A security policy should not include any exceptions.
- **C.** A security policy should not include a glossary.
- **D.** A security policy should not list all step-by-step measures that need to be taken.

15. The _____ contains the rules that must be followed.

- **A.** policy heading
- **B.** policy statement
- **C.** policy enforcement clause
- **D.** policy goals and objectives list

16. A policy should be considered _____.

- **A.** mandatory
- **B.** discretionary
- **C.** situational
- **D.** optional

17. Which of the following best describes policy definitions?

    A. A glossary of terms, abbreviations, and acronyms used in the document that the reader may be unfamiliar with
    B. A detailed list of the possible penalties associated with breaking rules set forth in the policy
    C. A list of all the members of the security policy creation team
    D. None of the above

18. The _____ contains the penalties that would apply if a portion of the security policy were to be ignored by an employee.

    A. policy heading
    B. policy statement
    C. policy enforcement clause
    D. policy statement of authority

19. What component of a security policy does the following phrase belong to? "Wireless networks are allowed only if they are separate and distinct from the corporate network."

    A. Introduction
    B. Administrative notation
    C. Policy heading
    D. Policy statement

20. There may be situations in which it is not possible to comply with a policy directive. Where should the exemption or waiver process be explained?

    A. Introduction
    B. The policy statement
    C. Policy enforcement clause
    D. Policy exceptions

21. The name of the person/group (for example, executive committee) that authorized the policy should be included in the _____.

    A. version control table or policy statement
    B. heading or policy statement
    C. policy statement or policy exceptions
    D. version control table or policy heading

22. When you're drafting a list of exceptions for a security policy, the language should _____.

    A. be as specific as possible
    B. be as vague as possible
    C. reference another, dedicated document
    D. None of the above

23. If supporting documentation would be of use to the reader, it should be _____.

    A. included in full in the policy document
    B. ignored because supporting documentation does not belong in a policy document
    C. listed in either the policy heading or administrative notation section
    D. included in a policy appendix

24. When writing a policy, standard, guideline, or procedure, you should use language that is _____.

    A. technical
    B. clear and concise
    C. legalese
    D. complex

25. Readers prefer plain language because it _____.

    A. helps them locate pertinent information
    B. helps them understand the information
    C. saves time
    D. All of the above

26. Which of the following is not a characteristic of plain language?

    A. Short sentences
    B. Using active voice
    C. Technical jargon
    D. Seven or fewer lines per paragraph

27. Which of the following is the best term to use when indicating a mandatory requirement?

    A. must
    B. shall
    C. should not
    D. may not

28. A company that uses the term "employees" to refer to workers who are on the company payroll should refer to them throughout their policies as _____.

    A. workforce members
    B. employees
    C. hired hands
    D. workers

29. Which of the following statements is true regarding policy definitions?

    A. They should be included and maintained in a separate document.
    B. The general rule is to include definitions for any topics except technical, legal, or regulatory language.
    C. The general rule of policy definitions is to include definitions for any instance of industry-specific, technical, legal, or regulatory language.
    D. They should be created before any policy or standards.

30. Even the best-written policy will fail if which of the following is true?

    A. The policy is too long.
    B. The policy is mandated by the government.
    C. The policy doesn't have the support of management.
    D. All of the above.

EXERCISES

EXERCISE 2.1: Creating Standards, Guidelines, and Procedures

The University System has a policy that states, "All students must comply with their campus attendance standard."

1. You are tasked with developing a standard that documents the mandatory requirements (for example, how many classes can be missed without penalty). Include at least four requirements.
2. Create a guideline to help students adhere to the standard you created.
3. Create a procedure for requesting exemptions to the policy.

EXERCISE 2.2: Writing Policy Statements

1. Who would be the target audience for a policy related to campus elections?
2. Keeping in mind the target audience, compose a policy statement related to campus elections.
3. Compose an enforcement clause.

EXERCISE 2.3: Writing a Policy Introduction

1. Write an introduction to the policy you created in Exercise 2.2.
2. Generally an introduction is signed by an authority. Who would be the appropriate party to sign the introduction?
3. Write an exception clause.

EXERCISE 2.4: Writing Policy Definitions

1. The purpose of policy definitions is to clarify ambiguous terms. If you were writing a policy for an on-campus student audience, what criteria would you use to determine which terms should have definitions?
2. What are some examples of terms you would define?

EXERCISE 2.5: Understanding Baselines

The goal of this exercise is to understand what baselines are, why they are important, and the different types of baselines.

1. Read articles or watch tutorials on the importance of baselines in IT security.
2. Reflect on how baselines can contribute to uniformity and security in various IT environments.
3. Explore different tools and methodologies for baseline management across platforms such as Windows, Linux, and network devices.
4. Create a detailed security baseline for a chosen IT environment. Choose an IT environment that you are familiar with or interested in, such as Windows desktops, Linux servers, or network routers.
5. Document the standard configurations for the system.
6. Define appropriate security policies including password policies and security protocols. List approved software and version numbers. Outline procedures for regular updates and patches.
7. Compare your baseline with existing standards or best practices found in your research to evaluate its completeness and robustness.

PROJECTS

PROJECT 2.1: Comparing Security Policy Templates

1. Search online for "cybersecurity policy templates."
2. Read the documents and compare them.
3. Identify the policy components that were covered in this chapter.
4. Search for a real-world policy, such as Tufts University's Two-factor Authentication Policy, at https://it.tufts.edu/univ-pol.
5. Choose a couple terms in the policy that are not defined in the policy definitions section and write a definition for each.

PROJECT 2.2: Researching New York City's AI Bias Law

The objective of this project is to research the requirements, implications, and real-world application of New York City's AI Bias Law in hiring practices and why it was failing after being enacted.

PART 1: Background Research

Goal: Gain a foundational understanding of the AI Bias Law and its objectives.

1. Research and read articles, official documents, and other credible sources detailing New York City's AI Bias Law. Focus on understanding the definitions of Automated Employment Decision Tools (AEDTs) and the scope of the law.
2. Summarize the key elements of the law:
   - What are AEDTs?
   - What requirements does the law impose on employers using these tools?
   - What are the intended outcomes of the law?

PART 2: Exploring Implications and Challenges

Goal: Analyze the potential impacts of the law on employers and job seekers, and identify challenges in its implementation.

1. Consider the implications for employers in terms of compliance costs and changes to hiring practices. Reflect on how the law affects job seekers, especially those from marginalized groups.
2. Investigate any reported difficulties or controversies associated with implementing the law. Consider technical, legal, and ethical challenges.
3. Identify any criticisms or support from various stakeholders including businesses, advocacy groups, and legal experts.

4. Examine how companies have responded to the law and the real-world effectiveness of such regulations.
5. Choose one or more companies that have implemented measures to comply with the AI Bias Law. If specific company examples are scarce, consider hypothetical scenarios based on industry standards.
6. Analyze the steps these companies have taken to audit their AEDTs.
7. Evaluate the transparency of the published audit results and any actions taken based on those results.
8. Write a detailed report on your findings, highlighting effective practices and areas where companies may fall short in compliance.

PROJECT 2.3: Testing the Clarity of a Policy Document

1. Locate your school's cybersecurity policy. (It may have a different name.)
2. Select a section of the policy and use the U.S. Army's Clarity Index to evaluate the ease of reading. (See the "In Practice: U.S. Army Clarity Index" sidebar for instructions.)
3. Explain how you would make the policy more readable.

Case Study

Clean Up the Library Lobby

The library includes the following exhibition policy:

> Requests to utilize the entrance area at the library for the purpose of displaying posters and leaflets give rise to the question of the origin, source, and validity of the material to be displayed. Posters, leaflets, and other display materials issued by the Office of Campus Security, Office of Student Life, the Health Center, and other authoritative bodies are usually displayed in libraries, but items of a fractious or controversial kind, while not necessarily excluded, are considered individually.

The lobby of the school library is a mess. Plastered on the walls are notes, posters, and cards of all sizes and shapes. It is impossible to tell current from outdated messages. It is obvious that no one is paying any attention to the library exhibition policy. You have been asked to evaluate the policy and make the changes needed to achieve compliance.

1. Consider your audience. Rewrite the policy using plain language guidelines. You may encounter resistance to modifying the policy, so document the reason for each change, such as changing passive voice to active voice, eliminating redundant modifiers, and shortening sentences.

2. Expand the policy document to include goals and objectives, exceptions, and a policy enforcement clause.
3. Propose standards and guidelines to support the policy.
4. Propose how you would suggest introducing the policy, standards, and guidelines to the campus community.

Reference

1. Baldwin, C., *Plain Language and the Document Revolution*. Lamplighter, 1999.

Regulations Cited

"Executive Order—Improving Government Regulations," accessed April 2024, https://www.presidency.ucsb.edu/ws/?pid=30539.

"A History of Plain Language in the Government," accessed April 2024, https://www.plainlanguage.gov/about/history/.

"Executive Order 13563—Improving Regulation and Regulatory Review," accessed April 2024, https://obamawhitehouse.archives.gov/the-press-office/2011/01/18/executive-order-13563-improving-regulation-and-regulatory-review.

"Public Law 111-274—Oct. 13, 2010 [Plain Writing Act]," accessed April 2024, https://www.govinfo.gov/content/pkg/PLAW-111publ274/pdf/PLAW-111publ274.pdf.

Additional Reference

Krause, M., and H. F. Tipton. *Information Security Management Handbook*, 5th ed. CRC Press, 2004.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z