# CHAPTER 1: POLICY DEFINED

## Chapter 01: Multiple Choice:

**1.** Which of the following is NOT a state in which information exists?
- A. stored
- B. processed
- C. factored
- D. transmitted

**2.** Why is it important to consistently enforce policy, and not "go easy on someone"?
- A. The welfare of the overall organization is more important than the individual's
- B. Playing favorites creates resentment
- C. It is easier to defend in court
- D. Policies should never be broken

**3.** Which of the following is LEAST likely to lead to employees accepting and following policy?
- A. Introduce policies through training programs
- B. Make policy compliance part of the job descriptions
- C. Consistently enforce policies
- D. Seek input from the organization when developing policies

**4.** Why is it important to prepare written policies?
- A. So the policies can be communicated more easily
- B. This helps to ensure consistency
- C. A policy is part of the corporate culture
- D. It is required by law

**5.** Why is it important for leadership to set a tone of compliance with policy?
- A. The rest of the organization feels better about following the rules
- B. It is part of their job
- C. Management are some of the worst offenders
- D. They are the ones that write the policies

**6.** When should information security policies, procedures, standards, and guidelines be revisited?
- A. As indicated in the policy
- B. Never; once they are written and published, they must be adhered to
- C. Annually
- D. When dictated by change drivers

**7.** Which is the best way to foster acceptance of a new policy?
- A. Involve people in policy development by conducting interviews
- B. Give everyone a copy of the policy after it is written
- C. Ensure it is detailed enough that everyone will understand it
- D. Hold meetings to explain it

**8.** Which is a two wall challenge?
- A. Screened-subnet firewall
- B. Requiring security badges at both doors to a room
- C. Lack of awareness, and the lack of awareness about the lack of awareness
- D. When two policies conflict with each other

 

**9.** Which is the preferred approach to organizing information security policies, procedures, standards, and guidelines?

A. Combine policies and procedures
B. Keep the policy documents separate from the procedures, standards, and guidelines
C. Combine standards and guidelines
D. Keep them all separate

**10.** Why do we need the Graham-Leach-Bliley Act (GLBA)?

A. The information banks possess can be identifiable and whole in regard to any customer
B. It protects banks from lawsuits due to a lack of fair treatment of employees
C. Health care organizations must safeguard private health care information from disclosure
D. Businesses need expert advice to achieve and sustain compliance

**11.** What should be the consequences of information security policy violations?

A. Always up to, and including, termination
B. Immediate revocation of all user privileges
C. Commensurate with the criticality of information the policy was written to protect
D. Violations should be cited in the person's annual performance review

**12.** Leadership by setting the example, or "do as I do", is considered:

A. Ineffective in a high-tech company
B. The same as "management by walking around"
C. Something that should only be employed when information security policies are new
D. The most effective leadership style, especially in relation to information security

**13.** Why is it important to remind people about best practice information security behaviors?

A. This approach is a mandatory requirement of information security policies
B. Reminders are the least expensive way to ensure compliance with policies
C. It ensures they are aware that management is watching them
D. Reminders reinforce their knowledge, and help them better understand expectations

**14.** Which is the worst that may happen if information security policies are out of date, or address technologies no longer used in the organization?

A. People may take the policies less seriously, or dismiss them entirely
B. Executive management may become upset
C. The company may incur unnecessary costs to change them
D. People may not know which policy applies

**15.** Which is the best goal for a new policy?

A. Accurately reflect the current technology environment
B. Comply with applicable government policy
C. Secure and protect assets from foreseeable harm, and provide flexibility for the unforeseen
D. Approved by management, and understood by everyone

**16.** Which part of the U.S. Constitution is analogous to the first approved version of a new information security policy?

A. amendments
B. articles
C. the Torah
D. the Bill of Rights

**17.** In what way are the Torah and the U.S. Constitution like information security policies?

A. They contain articles and amendments
B. They include business rules
C. They define the role of government in our daily lives
D. They serve as rules to guide behavior in support of organizational goals

**18.** What issue is addressed by both the Bible and corporate policies?

A. People tend to forget things if they are not periodically reminded of their obligations
B. Without common rules, people may adopt common behaviors and choices that make the overall group less stable
C. Stealing
D. The behavior of people in power

## Fill in the Blank:

**19.** An information security gap exists when users share account names and passwords with each other.

**20.** An organization which does not enforce policy is said to have paper only policies.

**21.** The Board of Directors are either elected or chosen to direct the affairs of a corporation, and are responsible for providing oversight of the information security program.

**22.** According to HIPAA, private health care information must remain protected from damage, misuse, and disclosure.

**23.** The U.S. Constitution's amendments are the built-in framework that makes it possible to change the document, while still adhering to its original intent.

## Matching:

**24.** Match each role with its responsibilities to the right:

| | |
|---|---|
| I. Board of Directors →**B** | A. Ensure that information security controls are functioning as intended |
| II. Information Owner →**C** | B. Approve written information security policies |
| III. Data Custodian →**D** | C. Establish the controls that provide information security |
| IV. ISO →**E** | D. Process and store information |
| V. Internal Auditor →**A** | E. Administer the information security function |

**Answer:** B C D E A **Reference:** Involving Those Who Know What Is Possible **Difficulty:** moderate

**25.** Match the following terms to their meanings:

| | |
|---|---|
| I. Foreign Policy →**E** | A. Policy adopted by society through legislative means to govern its people |
| II. Law →**A** | B. Civil or criminal; imposed for violations |
| III. Policy Area →**C** | C. A general topic, which relates to specific behavior and expectations |
| IV. Penalty →**B** | D. Standards for public and private education |
| V. Education Policy →**D** | E. Ways and means for one nation to deal with another |

**Answer:** E A C B D **Reference:** Defining the Role of Policy in Government **Difficulty:** moderate

## CHAPTER 2: THE ELEMENTS OF A POLICY

### Chapter 02: Multiple Choice:

**26.** What are the two schools of thought regarding policy format?
- A. A separate document for each policy, or one large document with multiple sections
- B. Use Microsoft Word, or Adobe Acrobat
- C. The ISO approach, or the OSI approach
- D. One large document with multiple sections or one large document

**27.** Where should the penalty for violating a policy be listed?
- A. In the first chapter of the Employee Handbook
- B. In the policy enforcement clause within the policy
- C. In the policy violation penalties document
- D. In the policy enforcement document

**28.** Which of the following are all federal regulations?
- A. Sarbanes-Oxley, IEEE 802.11, NIST 800-34
- B. GLBA, HIPAA, and Sarbanes-Oxley
- C. GLBA, HIPAA, and IEEE 802.11
- D. GLBA, NIST 800-34, and Sarbanes-Oxley

**29.** Which of the following is NOT a way in which the number of policy exceptions reflect on the quality of a policy?
- A. Too many exceptions to a valid rule in a policy may mean that there is a loophole in the policy.
- B. Too many exceptions to a rule in a policy may mean that the rule is inappropriate.
- C. Too many exceptions to a rule in a policy may mean that employees perceive the rule as unimportant.
- D. Too many exceptions to a valid rule may cause employees to feel that favoritism is being extended to some, but not all, employees

**30.** In what way is a speed limit like a standard?
- A. They are not alike at all
- B. A standard, like a speed limit, is always expressed in numeric form
- C. A speed limit, like a standard, is very definite, and required
- D. Both are suggested levels of performance

**31.** Which of the following is the best example of an acceptable password?
- A. T0yot@tRuck
- B. May12345
- C. FredD
- D. HappyDeyz

**32.** Which of the following is an outline of a complete policy?
- A. Purpose, Objectives, Policy, Exceptions, and Disciplinary Actions
- B. Objectives, Purpose, Policy, Exceptions, and Disciplinary Actions
- C. Objectives, Purpose, Audience, Policy, Exceptions, and Procedures
- D. Objectives, Purpose, Audience, Policy, Exceptions, and Disciplinary Actions

**33.** Which of the following is a good rule of thumb for including definitions in a policy?

A. Always include a definitions section at the end of a policy
B. Include definitions for any instance of non-standard language
C. Provide the definition of any non-standard word in parentheses after the word's first appearance
D. Cite sources of information about non-standard terms in the policy's bibliography

**34.** Which of the following is the best definition of a policy audience?

A. All employees granted unescorted access to the company's computer room
B. All headquarters employees
C. Any employee in the computer room
D. Only those employees in the computer room

**35.** Which of the following should you strive for in the policy statement, in order to have a well-written policy?

A. Contain areas that address every aspect of operations and information, and every area affecting the organization's information assets
B. Spell check the document to avoid typographical errors
C. Include applicable standards, guidelines, and procedures within the policy document
D. Describe everything in layman's terms, so that it is clear the policy is a statement of everyone's intent

**36.** Which of the following is true of procedures?

A. Procedures focus on sequential actions or steps, which are the instructions needed to carry out a policy statement.
B. Procedures must be changed every 30 days.
C. Procedures are a prerequisite to developing a policy; they must exist before you can write a policy.
D. Procedures are suggestions for the best way to accomplish a certain task.

**37.** In which of the following policy elements should the policy number appear?

A. Policy heading
B. Policy statement of purpose
C. Policy objectives
D. Statement of authority

**38.** Which of the following do the Graham-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) require in an organization's information security policy?

A. The date the policy was written and revised
B. A schedule for future policy review and revision
C. A statement with consequences of violating the policy
D. All of the above

**39.** Which of the following is true of policy elements?

A. They are only standards, guidelines, and procedures
B. Policy elements are an optional component of a policy
C. Best practice dictates that all policy elements should be included in the policy document itself
D. They depend on, and support each other, while supporting the document as a whole

**Answer:** D **Reference:** Introduction **Difficulty:** easy

**40.** Which of the following is NOT one of the common pitfalls encountered when policy companions (standards, guidelines, and procedures) are combined into the same document as the policy itself?
A. Difficult to implement
B. Difficult to manage
C. Difficult to update
D. Difficult to justify

**41.** Which of the following questions is answered by the policy objective?
A. Why
B. How
C. What
D. When

**42.** Where would you find the name of your company and the effective date of the policy you're looking at?
A. Policy heading
B. Policy objectives
C. Policy statement of purpose
D. Statement of authority

**43.** Which of the following is an easy mistake, which should be avoided when preparing the policy statement of purpose?
A. Attempt to get too detailed
B. Forget to include the signature line
C. Omit the effective date of the policy
D. Describe in broad terms how the policy will be implemented

**44.** Which of the following is NOT a way in which the policy definitions make the policy better?
A. Policy definitions enable the target audience to better understand the policy
B. Policy definitions help to provide a legal baseline
C. Policy definitions make the policy look like other official documents
D. Policy definitions make the policy document more efficient

**45.** The disciplinary process indicated in an information security policy enforcement clause usually includes which of the following most severe punishments?
A. Dismissal or criminal prosecution
B. Loss of one month's pay
C. Demotion to a lower level
D. Transfer to another division in the company

**46.** Which of the following is NOT something that a statement of authority tries to do?
A. Explain the organization's reason for writing the documents
B. Recruit readers and show what is expected of them as employees
C. Define what employees are expected to do in order to comply with the policies
D. Describe regulatory compliance responsibilities that the company has

**47.** Which of the following documents is likely to change most often?
A. Guidelines, because new improved best practices continually emerge
B. Standards, because they are specific to the technology platform in use

C. Procedures, because they are so detailed
D. Policies, because they reflect core values

**48.** Which of the following most likely be in the policy exceptions part of a company's policy that prohibits the use of modems?

A. All requests for modems must be approved by the Information Security department prior to installation
B. A modem inventory form must be sent to the Information Security department immediately following the installation of all new modems
C. Only Bell 202C modems may be installed
D. No modems whatsoever may be installed

**49.** Which of the following is MOST likely to reflect the policy audience for a corporate ethics policy at Acme Manufacturing?

A. All Acme Manufacturing employees, and all vendors and service providers
B. All full- and part-time employees of Acme Manufacturing and its subsidiaries
C. The Acme Manufacturing Board of Directors
D. The Finance, Human Resources, and Marketing departments of Acme Manufacturing

**50.** Which of the following is contained in the policy statement?

A. The rules for implementing the policy
B. The location of documents that explain the reasoning behind the rules
C. Sometimes the step-by-step procedures required to perform the tasks defined in the policy
D. All of the above

**51.** If a new United States federal information-sharing law is adopted, which of the following best represents a related information security policy statement of purpose?

A. Uphold the U.S. Constitution
B. Ensure compliance with federal law
C. Prevent personal information from being used for identity theft
D. Maintain individuals' right to privacy, as granted under the U.S. Constitution

**52.** If a new United States federal information-sharing law is adopted, which of the following best represents a related information security policy objective?

A. Ensure compliance with federal law
B. Obtain prior written approval from all individuals whose personal data is to be shared
C. Maintain individuals' right to privacy, as granted under the U.S. Constitution
D. Prevent personal information from being used for identity theft

**53.** Which of the following best describes the sequence of action steps posted on the front of an automated teller machine (ATM) at a bank?

A. Standards
B. Procedures
C. Guidelines
D. Policies

**54.** Which of the following best describes Guidelines?

A. Demands
B. Suggestions
C. Questions
D. Statements

**55.** If a policy refers the reader to another section for clarification of any instance of non-standard language, that other section would best be called which of the following?

A. Policy Definitions
B. Policy Header
C. Policy Enforcement Clause
D. Policy Exceptions

**56.** Which of the following best describes how the penalties defined in the Policy Enforcement Clause should relate to the infractions?

A. Any infraction should result in suspension or termination
B. The same penalty should apply each time an infraction occurs
C. The penalty should be proportional to the level of risk incurred as a result of the infraction
D. Penalties should be at the discretion of management

**57.** Which of the following best describes how policy exception requests should be handled?

A. Requestors should only be notified after their exception requests are approved
B. Requestors should always receive a response to any request, whether approved or not
C. Requestors should be notified why their exception requests were denied, so they can do a better job the next time
D. Requestors should be able to count on a seven-day turnaround on any policy exception request

**58.** Which of the following describes how much of the final policy document is typically made up of policy statements?

A. The policy statement is one section of the final policy document
B. Policy statements appear throughout the final policy document
C. Policy statements typically represent about 45% of the final policy document
D. The bulk of the final policy document is composed of policy statements

**59.** Which of the following best describes when the policy audience is most likely to include people outside the organization?

A. The policy audience needs to include people outside the organization whenever those people are involved with an aspect of the organization or its information
B. Any policy audience generally includes people outside the organization, because companies depend so heavily on outsourcing these days
C. People outside the organization should not be part of the policy audience, because there is no way to apply the policy enforcement clause against them
D. This is spelled out in the non-disclosure agreement

**60.** Which of the following best represents a Policy Statement of Purpose for a credit card company's Graham-Leach-Bliley Act compliance policy?

A. Comply with federal law, by mailing annual disclosures to customers
B. Mail annual disclosures to customers, and conduct annual training for employees
C. Comply with federal law, in order to protect the company's reputation
D. Protect customers' personal information

**61.** Which of the following parts of an organization's software policy would most likely indicate that any new software purchases be made only from the approved software products list?

A. Policy statement of purpose
B. Policy exceptions
C. Policy objective
D. Policy audience

**62.** Which of the following is the MOST important rule of thumb to follow when developing the policy heading?

A. The policy number must be included in the policy heading
B. Ensure its structure is scalable, so that it is able to accommodate changes in the future, without losing its original organization
C. Plan to spend the most time working on the policy heading; it is the most important part of the document
D. Ensure the policy heading contains all the same information as every other policy

**63.** Which of the following is true of the Statement of Authority?

A. It is usually not found in each individual policy, and serves as a preface to a group of policies and the entire information security program
B. It should strike fear into the hearts of all readers, in order to get them to take the policy seriously
C. It should contain very strict language, in order to impress people with its importance
D. It must appear in each individual policy, because it explains the company's motivation for developing the policies

**64.** In which of the following ways does understanding policy elements help you interpret your organization's information security policies?

A. Awareness of policy elements helps you determine the strength of the policy, and whether you should take it seriously
B. If you understand policy elements, you will be able to change the policies
C. Knowing the purpose and goal of each section of the policy can help you better understand the intent of the policy, as well as how the policy applies to you
D. You need to know the policy elements in order to determine which parts of the policy apply to you

**65.** If you are assigned to author your company's information security policies, which of the following is the MOST important thing to do first?

A. Look at all the other policies to get an idea of how they are written
B. Plan before you write
C. Determine when they are due
D. Express thanks for being given such a good assignment

**66.** The setup instructions that come in the box when you buy a new printer are an example of which of the following?

A. Standards
B. Procedures
C. Guidelines

 

D. Policies

**67.** The passage "In order to protect their home computers, remote users should consider installing anti-virus software, a firewall, and anti-spam filters" represents which of the following:

A. Procedures
B. Guidelines
C. Policy
D. Standards

**68.** In which of the following ways do password construction standards in a password policy make it better?

A. Standards suggest options for the best way to comply with the policy
B. Standards provide a permanent basis for the policy
C. Standards help to ensure consistency with minimum requirements
D. Standards indicate who is affected by the policy

**69.** Which of the following is a good way to help ensure that your company's information security policies represent best practices?

A. Base them on current industry standards for practices and technology
B. Provide little or no opportunity for policy exceptions to be granted
C. Copy key parts of similar policies you find on the Internet
D. Keep the suggested guidelines to a minimum, and focus on mandatory standards

**70.** When writing a new information security policy to cover data movement within your company, which of the following represents the BEST approach to take in order to ensure the policy will fulfill its intended purpose, help the policy audience understand what they need to do, and be sustainable?

A. Provide supporting documentation outside the policy document, in order to make it easier to implement, manage, and update
B. Follow existing standards, guidelines, and procedures as the policy
C. Develop a comprehensive policy, by including all applicable policy elements and supporting documentation in the policy document
D. Hold workshops to build employees' awareness of the policy after it is written and approved

**71.** Which of the following is the reason why United States government official communications about new federal laws frequently include references to other documents?

A. This approach is required by law
B. Congress must ensure that the new laws are comprehensive, so they can be defended in court
C. These references help those affected by the new laws gain a better understanding of what they need to do
D. It makes it easier to keep track of things

**72.** In which of the following ways does understanding policy elements enable the development of information security policies?

A. One cannot develop information security policies without an understanding of policy elements
B. Understanding policy elements enables us to break the policies down into their essential components, in order to more efficiently and effectively create usable policies

C. Information security policies must include all policy elements in order to be valid
D. It is necessary to understand policy elements in order to document which penalties apply for violation of information security policies

**73.** Which of the following is NOT true of policy elements?
A. Policy elements can be thought of as individual sections of the policy document
B. Standards, guidelines, and procedures are policy elements
C. Each policy element has its own specific purpose
D. Understanding policy elements helps you focus on the goal of each section of the policy, in order to be more consistent in how you write

**74.** Which of the following is an important function of the statement of authority?
A. It provides a bridge between an organization's core values and security strategies
B. It indicates who to talk to if you want to request a change in the policy
C. It describes the penalties for policy infractions
D. It references standards, guidelines, and procedures which the reader can consult for clarification of the policy

**75.** Which of the following is a reason why information security policy documents should include a version or change control number?
A. In order to maintain consistency
B. It is required by law
C. It can be a good way to promote that you wrote the policy
D. Information technology uses a lot of math

## Fill in the Blank:

**76.** The policy statement is the part of the document that is traditionally the one that constitutes the bulk of the final document known as the policy.

**77.** The policy objective states the goal of the policy, or what we are trying to achieve by implementing the policy.

**78.** A guideline suggests the best way to accomplish a certain task.

**79.** The Policy Enforcement Clause allows the organization to assert the seriousness of the policy.

**80.** Policy companions include specific standards, suggested guidelines, and sequential procedures.

## Matching:

**81.** Match each part of the policy statement with what it defines:

| | |
|---|---|
| I. goal →**B** | A. why |
| II. audience →**C** | B. what |
| III. purpose →**A** | C. who |

**Answer:** B C A **Reference:** Policy Statement **Difficulty:** easy

**82.** Match each of the following terms to its respective part of the policy excerpt that appears below:
"Fair business practices are a cornerstone of our company's corporate ethics program. In support of this goal, Acme Manufacturing will require all employees to decline all gifts or entertainment offered to them by vendors, and to report all offers to the Ethics Office. The purpose of this policy is to maintain the company's business ethics by clearly informing all employees of their obligations to be ethical in their business dealings on behalf of the company."

| | |
|---|---|
| I. What →**C** | A. Clearly inform all employees of their obligations |
| II. Why →**D** | B. All employees |
| III. How →**A** | C. Decline all offers of gifts or entertainment, and report all offers |
| IV. Who →**B** | D. Maintain the company's business ethics |

**Answer:** C D A B **Reference:** Policy Objectives, Policy Statement of Purpose **Difficulty:** moderate

**83.** Match the terms below to complete each cliché that applies to the policy enforcement clause:

| | |
|---|---|
| I. add →**C** | A. the language |
| II. walk →**D** | B. some muscle |
| III. live →**A** | C. some bite to your bark |
| IV. do →**E** | D. your talk |
| V. flex →**B** | E. what you say |

**Answer:** C D A E B **Reference:** Policy Enforcement Clause **Difficulty:** easy

## CHAPTER 3: INFORMATION SECURITY FRAMEWORK

### Chapter 03: Multiple Choice:

**84.** What does CIA stand for?
A. Confidentiality, Integrity and Authorization
B. Confidentiality, Integrity and Accountability
C. Confidentiality, Integrity and Authentication
D. Confidentiality, Integrity and Availability

**85.** The goal of protecting confidentiality is to
A. Prevent the unauthorized disclosure of sensitive information
B. Prevent the authorized disclosure of sensitive information
C. Prevent the unauthorized disclosure of public information
D. Prevent the authorized disclosure of public information.

**86.** Which of the following is NOT a threat to data confidentiality?
A. Hackers
B. Encryption
C. Improper access controls
D. Social engineering

**87.** What is shoulder surfing?
A. Conning someone into giving away their password
B. Looking at a person using their computer in hopes of viewing sensitive information
C. Another word for social engineering

D. Waiting for a user to leave their workstation and taking their place behind the keyboard

**88.** Which of the following is NOT an example of social engineering?
A. Calling an employee on the phone and impersonating an IT consultant to learn passwords
B. Running a password-cracking utility against a web server
C. Dressing up as UPS employee and gaining access to sensitive areas of a business
D. Posing as a potential customer in a Bank and gaining access to a computer terminal by pretending to need to send an email

**89.** Which of the following is NOT an example of malicious code?
A. Key logger
B. Virus
C. Worm
D. Solitaire

**90.** What is a valid definition of data integrity?
A. Knowing that the data on the screen is un-tampered with data
B. Data that is encrypted
C. Data that has not been accessed by unauthorized users
D. The knowledge that the data is transmitted in ciphertext only

**91.** Data integrity is
A. Protecting the data from intentional or accidental disclosure
B. Making sure the data is always available when legitimately needed
C. Protecting the data from intentional or accidental modification
D. Making sure the data is always transmitted in encrypted format

**92.** An employee accidentally makes changes to a company-owned file. This is known as a violation of
A. Data Confidentiality
B. Data Integrity
C. Data Availability
D. Dave Authorization

**93.** Which of the following is NOT a threat to data integrity?
A. Hackers
B. Improper access controls
C. Use of encrypted emails
D. Malicious code

**94.** Data availability is the assurance that
A. Only authorized users will gain access to a resource
B. All data stored on a hard drive is encrypted
C. All sensitive data stored on a hard drive is encrypted
D. Data and systems are accessible anytime they are needed

**95.** Guaranteed 99.999% uptime is an example of
A. Data integrity
B. Data authentication
C. Data confidentiality
D. Data availability

 

## Fill in the Blank:

**96.** Availability is the assurance that systems and data are accessible by authorized users when needed.

**97.** The service level agreement is a type of agreement between the service provider and a customer.

**98.** Networks are more vulnerable to availability threats than to the other components of the CIA triad.

**99.** The positive identification of the person or system seeking access is known as authentication.

**100.** Granting users and systems a predetermined level of access to information resources is known as authorization.

**101.** The logging of access and usage of information resources is known as accounting.

## Matching:

**102.** Match each topic with its definition to the right:

| | |
|---|---|
| I. Accountability →**B** | A. The logging of access and usage of information resources |
| II. Assurance →**C** | B. The process of tracing actions to their source |
| III. Authentication →**D** | C. The processes used to develop confidence that security measures are working |
| IV. Authorization →**E** | D. The positive identification of the person or system seeking access |
| V. Accounting →**A** | E. Granting users a predetermined level of access to information resources |

**Answer:** B C D E A **Reference:** The "Five As" of Information Security **Difficulty:** moderate

**103.** Match the following terms to their meanings:

| | |
|---|---|
| I. Confidential →**B** | A. Information available internally on a need to know basis |
| II. Sensitive →**A** | B. Information meant to be kept secret & restricted to a small circle of authorized |
| III. Public →**C** | C. Disclosure of this data would have no implication for the company |

**Answer:** B A C **Reference:** Classifying Data and Information **Difficulty:** moderate

**104.** Match the following terms to their meanings:

| | |
|---|---|
| I. Information ownership →**A** | A. Charged to those liable & responsible for protecting the information |
| II. Information custodians →**C** | B. Individuals with original responsibility for policies and practices |
| III. Information owners →**B** | C. Those charged with maintaining the systems that store, process and transmit information |

**Answer:** A C B **Reference:** Identifying Information Ownership Roles **Difficulty:** moderate

**105.** Match the following terms to their meanings:

| | |
|---|---|
| I. MAC →**A** | A. Classification system used by the federal government and the military |
| II. RBAC →**C** | B. Classification system where the owner decides who gets what level of access |
| III. DAC →**B** | C. Classification system that uses the employee's role to grant authorization |

**Answer:** A C B **Reference:** Classifying Data and Information **Difficulty:** moderate

**106.** Match the following ISO 17799:2000 domains to their definition:

| | |
|---|---|
| I. Security Policy →**B** | A. Design and maintenance of a secure environment to prevent damage and unauthorized access to the business premises |
| II. Organizational Security →**D** | B. Provides direction and support for the information security program |
| III. Asset Classification and Control →**C** | C. Involves creating an inventory of all data and data systems |
| IV. Personnel Security →**E** | D. Establish and support a management framework for information security |
| V. Physical and Environmental Security →**A** | E. Implement controls for secure hiring and termination of staff |

**Answer:** B D C E A **Reference:** Using the Ten Security Domains**Difficulty:** difficult

**107.** Match the following ISO 17799:2000 domains to their definition:

| | |
|---|---|
| I. Access Control →**B** | A. To ensure that the organization's information systems conform to local, national and international laws and mandates |
| II. Compliance →**A** | B. To prevent unauthorized access to data or information systems |
| III. Business Continuity Management →**D** | C. Provide security guidelines for creation of secure code and applications |
| IV. System Development & Maintenance →**C** | D. To protect the company from any situation that would result in the company not being able to perform its business tasks |
| V. Communications & Operations Management →**E** | E. To ensure the correct and secure operation of information processing facilities |

**Answer:** B A D C E **Reference:** Using the Ten Security Domains **Difficulty:** difficult

## CHAPTER 4: SECURITY POLICY DOCUMENTS AND ORGANIZATIONAL SECURITY POLICIES

### Chapter 04: Multiple Choice:

**108.** Who should issue the statement of authority?

A. The IT Manager
B. All the information owners
C. All the employees
D. The CEO, President or Chairman of the Board

**109.** This policy document is used to convey the organization's intention, objective, and commitment. It is known as:

A. The statement of authority
B. The Acceptable Use Policy
C. The affirmation agreement
D. The service level agreement

**110.** The statement of authority is also a statement of

A. Controls
B. Culture
C. Do's and Don'ts
D. Operations

**111.** This policy document is often referred to as a "policy about a policy". What is its real name?

A. Service level agreement
B. Security Policy Document Policy
C. Statement of authority
D. Acceptable use policy

**112.** Which of the following is NOT contained in the Security Policy Document Policy?

A. Who is in charge of designing the policy
B. What users may or may not do
C. Who is in charge of enforcing the policy
D. A statement about the need for information security policies

**113.** What is an "employee version" of the security policies?

A. A version written without the help of management
B. A version that does not contain the affirmation agreement
C. A version that does not contain the acceptable use policy
D. A succinct version of the comprehensive policy document that only includes information that pertains to the entire user base

**114.** The ISO Standard known as Managing Organizational Security includes several categories. Which of the following is NOT one of them?

A. Organizational Security Controls
B. Information Security Infrastructure
C. Identification of Risks from Third Parties
D. Security Requirements for Outsourcing

**115.** Which of the following federal regulations pertains to the medical field?

A. FERPA
B. GLBA
C. HIPAA
D. SOX

**116.** Which of the following federal regulations pertains to the educational field?

A. FERPA
B. GLBA
C. HIPAA
D. SOX

**117.** As it pertains to information security policies, what is the SOA?

A. Start of authority
B. Statement of Accountability
C. Statement of Authority
D. Summary of Authentication

## Fill in the Blank:

**118.** For a security policy to be successful, there must be a commitment from leadership.

**119.** The statement of authority is an introduction to the overall information security policy.

**120.** The goal of the statement of authority is to deliver a clear message about the importance of information security to all who read the document.

**121.** Creating a culture of security requires positive influences at multiple levels within the organization.

**122.** Security champions reinforce by example the message that security practices are important to the organization.

**123.** Change drivers are events within an organization that affect culture, procedures, activities, employee responsibilities, and relationships. They should trigger risks and vulnerability assessments.

**124.** When outsourcing work, pre-engagement due diligence investigations and clearly stated contractual obligations are extremely important

**125.** Acceptable use agreements are often called Employee Affirmation Agreements

## Matching:

**126.** Match the following federal regulations to their target audience:

| | |
|---|---|
| I. HIPAA →**B** | A. Educational Institutions |
| II. SOX →**D** | B. Healthcare service providers |
| III. FERPA →**A** | C. Financial institutions |
| IV. GLBA →**C** | D. Publicly traded companies |

**Answer:** B D A C **Reference:** Is There a Relationship Between Security **Difficulty:** moderate

**127.** Match the following terms to their meanings:

| | |
|---|---|
| I. Change driver →**C** | A. Introduction to the policy document |
| II. Acceptable use agreement →**D** | B. Policy about a policy |
| III. Statement of authority →**A** | C. any event that impacts culture, procedures and activities within an organization |
| IV. Security Policy Document Policy →**B** | D. Security Policy Document Policy D. List of actions that employees are not allowed to perform while using company- |

| | |
|---|---|
| | provided equipment |

**Answer:** C D A B **Reference:** Security Policy Document Policy **Difficulty:** moderate

## CHAPTER 5: ASSET CLASSIFICATION

### Chapter 05: Multiple Choice:

**128.** Which section of the ISO 17799 deals with asset classification?
- A. 2
- B. 3
- C. 4
- D. 5

**129.** Which of the following provide a way and place to process, store, transmit, and communicate information?
- A. Information systems
- B. Information assets
- C. Off-site storage solutions
- D. Outsourced storage solutions

**130.** Information systems are a combination of
- A. applications
- B. hardware and software
- C. controls and procedures
- D. policies and procedures

**131.** This classification level is used by the military for items "the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to National Security":
- A. For your eyes only
- B. Top Secret
- C. Secret
- D. Confidential

**132.** This classification level is used by the military for items "the unauthorized disclosure of which reasonably could be expected to cause serious damage to National Security":
- A. For your eyes only
- B. Top Secret
- C. Secret
- D. Confidential

**133.** This classification level is used by the military for items "the unauthorized disclosure of which reasonably could be expected to cause damage to National Security":
- A. For your eyes only
- B. Top Secret
- C. Secret
- D. Confidential

**134.** Which of the following is NOT a step used by hackers to infiltrate a network?
- A. Footprinting
- B. Data corruption
- C. scanning
- D. enumeration

**135.** Which data classification method is used by the US military?

A. DAC
B. RBAC
C. RDAC
D. MAC

**136.** When it comes to information security, what is labeling the vehicle for?

A. Communicating the sensitivity level
B. Communicating the access controls
C. Enforcing the access controls
D. Auditing the access controls

**137.** Information labels should be

A. encrypted
B. hidden
C. universally understandable
D. symbol-based only

**138.** Information needs to be handled according to

A. Its classification level
B. The statement of authority
C. The access controls set forth in the asset management policy
D. The access controls set forth in the affirmation agreement

**139.** Who is directly responsible for defining information asset protection?

A. The CEO/President/Chairman of the Board
B. The ISO
C. The Information Owner
D. The Information Custodian

**140.** Who is directly responsible for implementing information asset protection controls?

A. The CEO/President/Chairman of the Board
B. The ISO
C. The Information Owner
D. The Information Custodian

**141.** Who is directly responsible for using information asset in accordance with their classification levels?

A. The users
B. The ISO
C. The Information Owner
D. The Information Custodian

**142.** This is known as the process of upgrading the classification level of an information asset:

A. Declassification
B. Classification review
C. Reclassification
D. Classification Upgrade

**143.** This is known as the process of downgrading the classification level of an information asset:

A. Declassification

B. Classification review
C. Reclassification
D. Asset Publication

**144.** When calculating the value of an asset, which of the following is NOT a criterion?
A. Cost to acquire or develop asset
B. Cost to maintain and protect the asset
C. Cost to disclose the asset
D. Reputation

**145.** Hardware assets are
A. programs
B. code snippets
C. tangible pieces of equipment
D. Operating system

**146.** Which of the following is NOT an example of a software asset?
A. programs
B. code
C. wireless access point
D. Operating system

## Fill in the Blank:

**147.** Each asset, whether software or hardware, should have a unique identifier.

**148.** Best practices dictate that the organization chooses a naming convention for its assets and apply the standard consistently

**149.** An asset description should illustrate what an asset is used for.

**150.** For hardware devices, the manufacturer-assigned serial number should be recorded.

**151.** The physical address refers to the geographic location of the device itself, or the device that houses the information.

**152.** The logical address is where the asset can be found on the organization's network.

**153.** The controlling entity is the department or business what purchased or paid for the asset.

**154.** Criticality ratings provide a company with the basis on which to prioritize and allocate resources.

**155.** An information classification program lifecycle starts with assigning classification levels and ends with the process of declassification.

**156.** An information classification procedure is to characterize the criticality of the information system.

**157.** If the classification level of an asset must be upgraded, it is a process known as reclassification.

**158.** A(n) information asset is a definable piece of information, stored in any manner, which is recognized as having a value to the organization.

**159.** The first step to protecting assets is to create an asset inventory.

**160.** System impact refers to how vital this information asset is to business processes and/or customer service.

**161.** Protection level refers to the level of safeguards and/or controls required to protect the asset.

## Matching:

**162.** Match each concept with its definition:

| | |
|---|---|
| I. Information Labeling →**B** | A. Information needs to be used in accordance with its classification |
| II. Familiar labels →**C** | B. The vehicle for communicating the sensitivity level |
| III. Information handling →**A** | C. Classification labels should be easily understandable |

**Answer:** B C A **Reference:** Information Classification Labeling and Handling **Difficulty:** moderate

**163.** Commercial asset classification model: match the level with the definition:

| | |
|---|---|
| I. Confidential →**B** | A. business-centric information to be used internally only |
| II. Sensitive →**D** | B. Meant to be kept secret and restricted to only a small circle of employees |
| III. Restricted →**A** | C. information that does not require protection |
| IV. Public →**C** | D. Sometimes referred to as "personal" or "privileged" |

**Answer:** B D A C **Reference:** Commercial Classification Systems **Difficulty:** moderate

**164.** Match the following hacking steps to their meanings:

| | |
|---|---|
| I. footprinting →**C** | A. gathering specific network data such as user names and shares |
| II. scanning →**D** | B. launching an exploit |
| III. enumerating →**A** | C. process of accumulating data regarding a specific logical or physical target |
| IV. attacking →**B** | D. process of identifying vulnerabilities on a target network/host |

**Answer:** C D A B **Reference:** Commercial Classification Systems **Difficulty:** moderate

**165.** Commercial asset classification model: match the level with the definition.

| | |
|---|---|
| I Top Secret →**B** | A. disclosure could cause serious damage to National Security |
| II. Secret →**A** | B. disclosure could cause exceptionally grave damage to National Security |
| III. Confidential →**D** | C. disclosure would cause no damage to National Security |
| IV. Unclassified →**C** | D. disclosure could cause damage to National Security |

**Answer:** B A D C **Reference:** Government and Military Classification Systems

**166.** Match the assets with their corresponding examples:

| | |
|---|---|
| I Databases →**B** | A. Drawings, schematics, patents |
| II. Data files →**D** | B. Information about customers, personnel, and/or finances |
| III. Intellectual Property →**A** | C. Detailed instructions on how to perform various activities |
| IV. Research documentation →**E** | D. Transactional data giving up-to-date information about each event |
| V. Operational procedures →**C** | E. Proprietary information based on experimentation |

**Answer:** B D A E C **Reference:** What Are We Trying to Protect? **Difficulty:** moderate

## CHAPTER 6: PERSONNEL SECURITY

### Chapter 05: Multiple Choice:

**167.** Which section of the ISO 17799 deals with personnel security?
- A. 3
- B. 4
- C. 5
- D. 6

**168.** A job description should NOT provide which of the following types of information?
- A. The mission of the organization
- B. The responsibilities of the position
- C. Expectations regarding confidentiality
- D. Systems and software used for security

**169.** The age group most inclined to use an online job search is
- A. 30 to 49
- B. 18 to 29
- C. 50 to 64
- D. 33% of persons across all age groups use online job searching

**170.** A security clearance investigation does NOT involve research into a person's
- A. character
- B. reliability
- C. family connections
- D. trustworthiness

**171.** Which of the following are types of background checks?
- A. credit history
- B. criminal history
- C. license verification
- D. all of the above

**172.** Which of the following information about a person cannot be used to influence a hiring decision?
- A. educational credentials
- B. filing of a Workers' Compensation claim
- C. negative credit history
- D. relevant certifications

**173.** Which of the following is a component of an affirmation agreement?
- A. statement of authority
- B. background check
- C. job description
- D. credit history

**174.** Which of the following is NOT a type of employee agreement?
- A. acceptable use agreement
- B. employee information security affirmation agreement

C. certification maintenance agreement
D. confidentiality agreement

**175.** Which of the following are components of a good security incident reporting program?
A. training users to recognize suspicious incidents
B. providing follow-through and feedback
C. establishing a system for reporting incidents
D. all of the above

**176.** An information security affirmation agreement would be likely to cover the use of
A. e-mail
B. office supplies
C. parking
D. paid time off

## Fill in the Blank:

**177.** Overly informative job postings provide information that may be used in social engineering attacks.

**178.** A(n) job candidate should never be allowed to tour the facility.

**179.** The organization of information assets according to their sensitivity to disclosure is called information classification.

**180.** criticality is the ranking of information assets in terms of their importance.

**181.** The government assigns a clearance level to its personnel based on preset criteria and a background check.

**182.** Confidentiality agreements help to protect patent rights.

**183.** An event that threatens information or an information system is called a(n) security incident.

**184.** A(n) acceptable use agreement simply covers the rules for the proper use of information systems.

## Matching:

**185.** Match each type of employee agreement with its description:

| | |
|---|---|
| I. Confidentiality agreement →**B** | A. Teaches the importance of security and instills organizational values |
| II. Acceptable use agreement →**C** | B. Protects against unauthorized disclosure of information |
| III. Employee information security affirmation agreement →**A** | C. Focuses on proper use of information systems |

**Answer:** B C A **Reference:** The Importance of Employee Agreements **Difficulty:** easy

**186.** Match the following terms with their relationship to personnel security:

| | |
|---|---|
| I. Job description →**B** | A. Scrutiny before hiring |

| | |
|---|---|
| II. Interview →**C** | B. Reaches a wide audience of potential intruders |
| III. Background check →**A** | C. May unintentionally provide too much information |
| IV. Employee agreement →**D** | D. Establishes definitions for handling information |

**Answer:** B C A D **Reference:** The Importance of Employee Agreements **Difficulty:** moderate

**187.** Match each of the following with its example:

| | |
|---|---|
| I. Security education →**C** | A. posters reminding users to report security breaches |
| II. Security training →**B** | B. a presentation on creating good passwords |
| III. Security awareness →**A** | C. recertification training for the network administrator |

**Answer:** C B A **Reference:** SETA for All **Difficulty:** moderate

# Instructor's Manual Materials to Accompany
## SECURITY PROGRAM AND POLICIES

# CHAPTER 1
## UNDERSTANDING POLICY

## Key Terms

**Asset:** A resource with value.

**Corporate culture:** The shared attitudes, values, goals, and practices that characterize a company or organization.

**Guiding principles:** Synthesize the fundamental philosophy or beliefs of an organization.

**Information security policy:** A policy that defines how an organization plans to protect its tangible and intangible information assets and ensure compliance with legal and regulatory requirements.

**Policy:** A set of rules combined to create a management framework that dictates how an organization will function.

**Regulation:** Intervention with the purpose of either restraining or causing a specific set of uniform actions.

## TEACHING NOTES

I. Defining Policy

**Teaching Tips:** Emphasize that the key to writing policies lies in knowing what is protected and where it exists. Information security policy should secure information in three distinct states: stored, processed, and transmitted. Information in these states resides in information technology systems, on paper, and in human brains.

In class, have students discuss what should be in a policy for a veterinarian's office. Point out to students that class suggestions and comments center around what information needs to be protected (for example, account balances, credit card numbers, customer list, and appointment schedules) and where the information resides.

II. Defining the Role of Policy in Corporate Culture

**Teaching Tips:** Without policies, it would be almost impossible to organize any group for any reason and for any length of time. Government policy can, in turn, require businesses to create their own policy to achieve and sustain compliance.

 

The function of well-written information security policies is to protect the organization, its employees, its customers, and also vendors and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information.

III. Understanding What Make a Policy Successful

**Teaching Tips:** A successful policy should be supported by management, applicable to the organization, should make sense to the people it applies to, can be successfully implemented, can be changed when needed, can be enforced when needed, and includes all relevant parties.

IV. Understanding the Role of Government in Policy

**Teaching Tips:** Government intervention is required to protect its critical infrastructures and citizens. Examples of government information security-related legislation are the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA). States also play an important role is passing legislation when comprehensive national standards do not exists. The California Security Breach Information Act and the Massachusetts Standards for the Protection of Personal Information are two such examples.

V. Information Security Policy Lifecycle

**Teaching Tips:** Regardless of the type of policy, its success depends on how the organization approaches the process of development, publishing, adopting and reviewing the policy.

Policy development

**Teaching Tips:** There are six main tasks involved in policy development: planning, researching, writing, vetting, approving, and authorizing.

Policy Publication

**Teaching Tips:** Policies should be communicated and made available to all parties they apply to. The company should provide training to reinforce the policies. Creating a culture of compliance can ensure all parties understand the importance of the policy and actively support it.

Policy Adoption

**Teaching Tips:** The policy is implemented, monitored, and enforced.

Policy Review

**Teaching Tips:** Policies are reviewed annually and outdated policies are updated or retired.

 

## PROJECTS/EXERCISES

I. **Discussion Questions**

A. Discussion Question 1

In addition to the Bible and the U.S. Constitution, identify another written policy that had (or still has) a profound effect on societies across the globe, including our own.

Answer: Students' answers will vary. An acceptable policy should have been created out of a perceived need to guide human behavior in foreseeable circumstances, and even to guide human behavior when circumstances could not be or were not foreseen.

B. Discussion Question 2

How do policies communicate corporate culture?

Answer: Corporate culture can be defined as the shared attitudes, values, goals, and practices that characterize a company or corporation. These attitudes, values, goals, and practices are communicated to all the organization's employees, vendors, partners, and customers with policies that support organizational goals and provide expectations to help sustain consistency in the organization's services and products.

## CHAPTER REVIEW/ANSWERS TO TEST YOUR SKILLS

### MULTIPLE CHOICE

1. Policies define which of the following?

   D. All the above

2. Without policy, human beings would live in a state of

   A. Chaos

3. A guiding principle is best described as which of the following?

   B. A fundamental philosophy or belief

4. Which of the following best describes corporate culture?

   A. Shared attitudes, values, and goals

5. Which of the following is a true statement?

   B. Guiding principles set the tone for a corporate culture.

6. Which of the following best describes the role of policy?

D. All the above

7. An information security policy is a directive that defines which of the following?

C. How an organization protects information assets and systems

8. Which of the following is not an example of an information asset?

D. Building graffiti

9. What are the seven characteristics of a successful policy?

B. Endorsed, relevant, realistic, attainable, adaptable, enforceable, and inclusive

10. A policy that has been endorsed has the support of which of the following?

D. Management

11. Who should always be exempt from policy requirements?

C. No one

12. "Attainable" means that the policy _____.

A. Can be successfully implemented

13. Which of the following statements is always true?

C. Policies should be adaptable.

14. If a policy is violated and there is no consequence, the policy is considered to be which of the following?

A. Meaningless

15. Who must approve the retirement of a policy?

C. Executive management or the Board of Directors

16. Which of the following sectors is not considered part of the "critical infrastructure"? D. Chemical industry

17. Which term best describes government intervention with the purpose of causing a specific set of actions?

C. Regulation

18. The objectives of GLBA and HIPAA, respectively, are to protect _____.

A. Financial and medical records

19. Which of the following states was the first to enact consumer breach notification?

D. California

20. In 2010, Massachusetts became the first state in the nation to require _____.

 

B. Minimum standards for the protection of personally identifiable information of Massachusetts residents

21. Which of the following terms best describes the process of developing, publishing, adopting, and reviewing a policy?

D. Policy lifecycle

22. Who should be involved in the process of developing policies?

C. Personnel throughout the company

23. Which of the following does *not* happen in the policy development phase?

B. Enforcement

24. Which of the following occurs in the policy publication phase?

D. All the above

25. Normative integration is the goal of the adoption phase. This means _____.

C. The policy becomes expected behavior; all others being deviant.

26. How often should policies be reviewed?

D. At least annually or sooner if there is a significant change

27. Which of the following phrases best describes the concept of "championing a policy"?

A. A willingness to lead by example, encourage, and educate

28. Which of the following phrases best describes the philosophy of "honoring the public trust"?

C. Being a careful steward of information in your care

29. Who should authorize policies?

A. Directors or executive management

30. Which of the following statements is *not* an objective of information security?

D. To protect information and information systems from authorized users

 

# CHAPTER 2
# POLICY ELEMENTS AND STYLE

## KEY TERMS

**Guidelines:** Similar to suggestions for the best way to accomplish a certain task. They are more dynamic than the other components of a policy and are therefore edited more often.

**Plain language:** The simplest, most straightforward way to express an idea.

**Policy audience:** That portion of an organization directly concerned by the policy. This can range from a couple people to the entire organization. It may also refer to members of the "extended" organization, such as temporary employees and third-party consultants.

**Policy definitions:** Terms that define and clarify terminology used in the policy.

**Policy enforcement clause:** The part of the policy where sanctions for failure to comply with the policy are defined.

**Policy exceptions:** Defined exceptions to a written and implemented policy.

**Policy heading:** Contains all the logistical information regarding a specific policy area, such as security domain section, subsection, policy number, the name of the organization and of the document, the change control documentation or number, and the signing authority.

**Policy objective:** States what the organization is striving to achieve by implementing the policy.

**Policy statement:** Focuses on the specifics or details of the policy.

**Procedure:** Provides a method by which a policy is accomplished. Procedures provide the instructions necessary to carry out a policy statement.

**Standards:** Specific minimum requirements in policies. Standards are definite and required.

## TEACHING NOTES

I. Defining Policy Hierarchy: Standards, Baselines, Guidelines, and Procedures

**Teaching Tips:** Explain to students that because standards, baselines, guidelines, and procedures change far more often than policies, these should be separated from the policy document.

Standards

**Teaching Tips:** Standards dictate specific minimum requirements in a policy.

Baselines

 

**Teaching Tips:** An aggregate of implementation standards and security controls for a specific category or grouping. For example, a baseline can be created for all users using smartphones or all users connecting to the network through a VPN.

Guidelines

**Teaching Tips:** Guidelines are best thought of as suggestions for the best way to help people conform to the standards. Guidelines are likely to change more often than any other element in this family of documents.

Procedures

**Teaching Tips:** Procedures are the instructions necessary to carry out a policy statement. They focus on actions or steps, and there is usually a starting point and an ending point to that action. Four commonly used types are simple step, hierarchical, graphic, and flowchart.

II. Developing a Policy Style and Format

**Teaching Tips:** You need to know your intended audience and write in a way that is relevant and understandable for that audience. Follow the plain language techniques when writing policy documents.

Plan Before You Write

**Teaching Tips:** Policy format varies. Each policy can be written as a discrete document, called a singular policy, or one large policy document with multiple sections, called a consolidated policy section. Discrete documents offer the advantages of being short, clean, and crisp, and well targeted to the intended audience.

III. Defining Policy Components

**Teaching Tips:** The key to successful policy writing is to understand the goal of each section and to be consistent in how you write.

Version Control

**Teaching Tips:** Version control is used to keep track of any changes to the policy, including who authorized and made the changes and what is the effective date.

Introduction

**Teaching Tips:** The statement of authority serves as a preface to a group of information security policies and introduces the policies by presenting the thought process behind the actual policies to the reader. The statement of authority also usually attempts to "recruit" readers and show them what is expected of them as employees.

Policy Headings

**Teaching Tips:** A policy heading contains all the technical details relevant to a policy, such as version number, identity of the author(s), date of creation, and more.

Policy Goals and Objectives

**Teaching Tips:** The policy objective states *what* (not the why or how) we are trying to achieve by implementing the policy. One policy can feature multiple objectives.

 

Policy Statement

**Teaching Tips:** The policy statement focuses on the specifics of how the policy will be implemented, in other words, the rules. The policy will also reference the standards, procedures, and guidelines (all separate documents) that have been created to support all the rules that make up the policy.

Policy Exceptions

**Teaching Tips:** Keep the number of exceptions low. Language used when creating an exception must be clear, concise, and indicate a process by which exceptions may be granted. The criteria or conditions for exceptions should not be detailed in the policy, only the method or process for requesting an exception.

Policy Enforcement Clause

**Teaching Tips:** The only way to enforce the policy rules is to include the penalty for ignoring the rules in the same document. Do not list every possible punishment for every possible violation. Simply indicate a disciplinary process and list the most severe punishment, which usually includes dismissal or criminal prosecution.

Administrative Notations

**Teaching Tip:** It is used to provide a reference to an internal resource or to an external policy or regulation.

Policy Definitions

**Teaching Tips:** Include definitions for any instance of nonstandard language. When choosing which words will be defined, do not look only at those that could clearly be unknown by the target audience, but also include those that should be defined to remove any and all ambiguity.

# PROJECTS/EXERCISES

## I. Discussion Questions

### A. Discussion Question 1

What is the difference between a policy objective and a policy purpose?

Answer: Students' answers will vary. Essentially, the policy objective is to achieve a broad goal to more efficiently protect the company. The policy purpose explains how the company will protect itself from specific threats using the actual rules of the policy.

### B. Discussion Question 2

Why are policy definitions an important part of any policy?

Answer: Student answers should focus on the use of definitions to enhance understanding of the policy and the need to define a target audience. Another important reason for definitions is to remove all ambiguity from the policy. A security policy should be viewed as a legal document and crafted carefully.

 

## CHAPTER REVIEW/ANSWERS TO TEST YOUR SKILLS

**MULTIPLE CHOICE**

1. The policy hierarchy is the relationships between which of the following?

   B. Guiding principles, standards, guidelines, and procedures

2. Which of the following statements best describes the purpose of a standard?

   C. To dictate mandatory requirements

3. Which of the following statements best describes the purpose of a guideline?

   D. To make suggestions

4. Which of the following statements best describes the purpose of a baseline?

   **B.** To ensure uniformity across a similar set of devices

**5.** Simple Step, Hierarchical, Graphic, and Flowchart are examples of which of the following formats?

   **C.** Procedure

**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 timeframe, usually with defined stages and with designated resources?

   **A.** Plan

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

   **C.** You may end up with too many policies to maintain.

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

   **D.** The potential size of the document.

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

   **B.** False

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

   **D.** All the above

**11.** Which of the following is not a policy introduction objective?

   **B.** To provide explicit instructions on how to comply with the policy

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

   **B.** Policy Heading

 

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

**C.** Policy goals and objectives

**14.** Which of the following statements is true?

**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.

**B.** Policy statement

**16.** A policy should be considered _____.

**A.** Mandatory

**17.** Which of the following best describes policy definitions?

**A.** A glossary of terms used

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

**C.** Policy enforcement clause

**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."

**D.** The 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

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

**D.** The version control table or the policy heading

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

**A.** Be as specific as possible

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

**C.** Listed in either the Policy Heading or Administrative Notation section

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

**B.** Clear and concise

**25.** Readers prefer "plain language" because it _____.

**D.** All the above

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

**C.** Technical jargon

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

**A.** Must

**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 _____.

**B.** Employees

**29.** "The ball was thrown by Sam to Sally" is a passive sentence. Which of the following sentences represents an active version of this sentence?

**C.** Sam threw the ball to Sally.

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

**C.** The policy doesn't have the support of management.

# CHAPTER 3
# INFORMATION SECURITY FRAMEWORK

## KEY TERMS

**Accountability:** The process of tracing actions to their source. One of the "Five A's" of information security.

**Accounting:** The process of logging of access and usage of information or resources. One of the "Five A's" of information security.

**Assurance:** Measurement of confidence in a control or activity. One of the "Five A's" of information security.

**Authentication:** The process of confirming an identity. One of the "Five A's" of information security.

**Authorization:** The process of granting access after proper identification and authentication. One of the "Five A's" of information security.

**Availability:** The assurance that systems and information are accessible by authorized users when needed.

**CIA Triad:** The three tenets of information security: confidentiality, integrity, and availability.

**Confidentiality:** The protection of information from unauthorized people, resources, and processes.

**Five A's:** The Five A's of information security are accountability, assurance, authentication, authorization, and accounting.

**Information custodians:** Individuals in charge of maintaining the infrastructure on which the actual information travels and is stored. In most company, the IT department typically will be the information custodians.

**Information owners:** Individuals responsible for protecting information.

**Integrity:** The protection of information or processes from intentional or accidental unauthorized modification.

**Service level agreement (SLA):** An agreement between a service provider and a customer that specifically addresses availability of services.

## TEACHING NOTES

I. Planning the Goals of an Information Security Program.

**Teaching Tips:** Help students realize that information security is not a "point-in-time" measurement but rather an ongoing process requiring vigilance and sustained effort. Then they will understand why it is important to write policies that facilitate consistency and sustainability.

What Is Confidentiality?

**Teaching Tips:** Have students brainstorm threats to confidentiality using the list on p. 68 as a starting point.

What Is Integrity?

**Teaching Tips:** Have students brainstorm threats to integrity using the list on p. 69 as a starting point. Ask students to look at both lists and describe the difference between threats to confidentiality and threats to integrity.

What Is Availability?

**Teaching Tips:** Have students brainstorm threats to availability using the list on p. 71 as a starting point. Ask students to compare and contrast threats to availability, confidentiality, and integrity. Which type of threat is most likely to occur? (Availability – hardware will fail.)

The "Five As" of Information Security: Some Other Meaningful Letters and What They Stand For

II. Identifying Information Ownership Roles

**Teaching Tips:** Have students discuss the difference between information owner and information custodian. Ask students to provide an example of each.

III. The ISO/IEC 27002:2013 Code of Standards for Information Security.

**Teaching Tips:** Explain the functions of NIST and ISO, and ask students to locate one document published from each of these organizations that deals with information security.

IV. Using the Security Domains of the ISO 27002:2013

**Teaching Tips:** The term "domain" may be confusing to students who think of a network domain or a web domain. Clearly define "domain" in this context (an ISO domain) as simply a category. Have students identify the ISO domains and the purpose of each domain.

## PROJECTS/EXERCISES

I. **Discussion Questions**

A. Discussion Question 1

How does the ISO 27002:2013 standard relate to an organization's information security policy?

Answer: Student answers will vary. The standard is a comprehensive set of information security recommendations comprising best practices in information security. As such, it provides a framework to help organizations of any size develop appropriate controls to maintain the confidentiality, integrity, and availability of information.

B. Discussion Question 2

Describe an effective policy.

Answer: Student answers will vary. For policies to be effective, they must be meaningful and relevant as well as appropriate to the size and complexity of the organization. The key is to understand what policy and control may be needed in any given environment and then develop, adopt, and implement the controls and policies that make sense for the organization.

## CHAPTER REVIEW/ANSWERS TO TEST YOUR SKILLS

### MULTIPLE CHOICE

1. Which of the following are the three principles in the CIA triad?

**C.** Confidentiality, integrity, availability

**2.** Which of the following is an example of acting upon the goal of integrity?

**C.** Ensuring that all modifications go through a change-control process

**3.** Which of the following is a control that relates to availability?

**A.** Disaster recovery site

**4.** Which of the following is an objective of confidentiality?

**A.** Protection from unauthorized access

**5.** As it pertains to information security, assurance is _____.

**B.** The processes, policies, and controls used to develop confidence that security measures are working as intended

**6.** Which of the following terms best describes the granting of users and systems a predetermined level of access to information resources?

**D.** Authorization

**7.** Which of the following statements identify threats to availability? (Select all that apply.)

**A.** Loss of processing capabilities due to natural disaster or human error

**C.** Loss of personnel due to accident

**8.** Which of the following terms best describes the logging of access and usage of information resources?

**C.** Accounting

**9.** Which of the following combination of terms best describes the Five A's of information security?

**C.** Accountability, assurance, authorization, authentication, accounting

**10.** An information owner is responsible for _____.

**B.** Protecting the information and the business results derived from use of that information

**11.** Which of the following terms best describes ISO?

**B.** International Organization for Standardization

**12.** Which of the following statements best describes opportunistic crime?

**C.** Crime that takes advantage of an identified weakness

**13.** Which of the following terms best describes the motivation for hactivism?

**B.** Political

**14.** The greater the criminal work factor, the _____

**A.** More time it takes

 

**15.** Which of the following terms best describes an attack whose purpose is to make a machine or network resource unavailable for its intended use?

**C.** Denial of service

**16.** Information custodians are responsible for _____

**E.** Implementing safeguards

**17.** The National Institute of Standards and Technology (NIST) is a(n) _____

**C.** U.S. government agency

**18.** The Internal Organization for Standardization (ISO) is _____

**D.** All the above

**19.** The current ISO family of standards that relates to information security is _____.

**C.** ISO/IEC 27000

**20.** Which of the following terms best describes the security domain that relates to determining the appropriate safeguards as it relates to the likelihood of a threat to an organization?

**D.** Risk assessment

**21.** Which of the following terms best describes the security domain that relates to how data is classified and valued?

**B.** Asset management

**22.** Which of the following terms best describes the security domain that includes HVAC, fire suppression, and secure offices?

**D.** Physical and environmental controls

**23.** Which of the following terms best describes the security domain that aligns most closely with the objective of confidentiality?

**A.** Access control

**24.** The primary objective of the _____ domain is to ensure conformance with GLBA, HIPAA, PCI/DSS, FERPA, and FISMA.

**B.** Compliance

**25.** Processes that include responding to a malware infection, conducting forensics investigations, and reporting breaches are included in the _____ domain.

**C.** Incident Management

**26.** Which of the following terms best describes a synonym for business continuity?

**C.** Availability

 

**27.** The _____ can be held legally responsible for the safeguarding of legally protected information.

**B.** Information owner

**28.** Personnel screening, acceptable use, confidentiality agreements, and training are controls that relate to the _____ domain.

**C.** Human Resources

**29.** Defining organizational roles, responsibilities, and authority relate to the _____ domain.

**C.** Governance

**30.** Which of the following security objectives is most important to an organization?

**D.** The answer may vary from organization to organization.

# CHAPTER 4
# GOVERNANCE AND RISK MANAGEMENT

## KEY TERMS

**Acceptable use agreement:** A document that supports the security policy and clearly dictates for all employees how they are expected to use information and information systems.

**Audit Report:** A formal opinion of the audit team based on a predefined scope and criteria.

**Change drivers:** Events that modify how a company does business.

**Information security audit:** A systematic evidence-based evaluation on how well the organization conforms to established criteria such as policies, regulatory requirements, and internationally recognized standards.

**Risk:** The potential of an undesirable or unfavorable outcome resulting from a given action, activity, and inaction.

**Risk assessment:** The process by which risks are identified and the impact of those risks determined.

**Risk management:** The process of determining an acceptable level or risk, identifying the level or risk for a given situation, and determining if the risk should be accepted or mitigated.

**Risk mitigation:** The process of reducing, sharing, transferring, or avoiding risk.

**Risk tolerance:** How much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit.

 

**Threat:** A potential danger to an asset or resource.

**Vulnerability:** A weakness that could be exploited by a threat source.

# TEACHING NOTES

I. Understanding Information Security Policies

**Teaching Tips:** Influencing and defining culture is the role of leadership, so the signer should be seen as both a leader and a decision maker. The signer should also be seen as in touch with day-to-day operations, yet have enough authority to enforce the policy. Change drivers should trigger risk and vulnerability assessments and ultimately a review of policies.

The Information Security Policy Document policy should reference the federal (and state) regulations the organization is subject to. Each individual policy should have a cross reference notation to the specific regulatory section.

The policy owner is not the final authority. Ownership translates into developing, maintaining, and reviewing the policies and companion documents.

II. Information Security Governance

**Teaching Tips:** Mention that the Board of Directors is usually responsible for overseeing the policy development. Effective security requires a distributed governance model with the active involvement of stakeholders, decision makers, and users.

III. Information Security Risk

**Teaching Tips:** Companies use risk assessment to calculate the level of risk. Explain that the company can decide to either accept the risk or mitigate the risk. To mitigate the risk the company can take one of the following four actions: risk reduction, risk sharing, risk transference, risk avoidance, or a combination of these actions. Ask students to explain each of these actions and discuss when to use each action. Ask students to identify the risks of using third parties.

# PROJECTS/EXERCISES

I. **Discussion Questions**

A. Discussion Question 1

Why should a statement of authority reflect the organization's culture?

Answer: Students' answers will vary. The SOA should be thought of as a teaching tool sprinkled with a motivational "pep talk," so the most effective communication will take into account the audience's background, education, experience, age, and even native language. Corporate culture can be defined as the shared attitudes, values, goals, and practices that characterize a company or corporation.

B. Discussion Question 2

 

Ideally, who is involved in designing and maintaining a secure organizational environment?

Answer: Students' answers will vary. This is a huge undertaking that requires input from professionals throughout an organization, including members of management, developers, network engineers and administrators, Human Resources, and legal and financial communities. Following the rules is possible only if the infrastructure is designed in such a way that following the rules is easy and doesn't hinder performance or productivity, which requires input from all levels of the organization.

## CHAPTER REVIEW/ANSWERS TO TEST YOUR SKILLS

### MULTIPLE CHOICE

1. When an information security program is said to be "strategically aligned," this indicates that _____.

**D.** All of the above

**2.** How often should information security policies be reviewed?

**C.** At a minimum, once a year and whenever there is a change trigger

**3.** Information security policies should be authorized by _____.

**A.** the Board of Directors (or equivalent)

**4.** Which of the following statements best describes policies?

**D.** Policies are the directives that codify organizational requirements.

**5.** Which of the following statements best represents the most compelling reason to have an employee version of the comprehensive information security policy?

**D.** The more understandable and relevant a policy is, the more likely users will positively respond to it.

**6.** Which of the following is a common element of all federal information security regulations?

**A.** Covered entities must have a written information security policy.

**7.** Organizations that choose to adopt the ISO 27002:2103 framework must _____.

**C.** Evaluate the applicability and customize as appropriate

**8.** Evidence-based techniques used by information security auditors include which of the following elements?

**B.** Structured interviews, observation, review of practices, and documentation sampling

**9.** Which of the following statements best describes independence in the context of auditing?

**C.** The auditor is not responsible for, benefited from, or in any way influenced by the audit target.

**10.** Which of the following states is *not* included in a CMM?

**A.** Average

**11.** Which of the following activities is not considered a governance activity?

**D.** Purchasing

**12.** To avoid conflict of interest, the CISO could report to which of the following individuals?

**C.** The Chief Financial Officer (CFO)

**13.** Which of the following statements best describes the role of the Information Security Steering Committee?

**B.** The committee serves in an advisory capacity.

**14.** Defining protection requirements is the responsibility of _____.

**C.** Data owners

**15.** Designating an individual or team to coordinate or manage information security is required by _____.

**D.** All of the above

**16.** Which of the following terms best describes the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or inaction?

**B.** Risk

**17.** Inherent risk is the state before _____.

**B.** security measures have been implemented

**18.** Which of the following terms best describes the natural, environmental, or human event or situation that has the potential for causing undesirable consequences or impact?

**C.** Threat

**19.** Which of the following terms best describes a disgruntled employee with intent to do harm?

**B.** Threat source

**20.** Which of the following activities is *not* considered an element of risk management?

**D.** Installing risk-mitigation safeguards

**21.** How much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit is known as _____.

**B.** risk tolerance

 

**22.** Which of the following statements best describes a vulnerability?

**A.** A vulnerability is a weakness that could be exploited by a threat source.

**23.** A control is a security measure that is designed to _____ a threat source.

**D.** All the above

**24.** Which of the following is not a risk-mitigation action?

**A.** Risk acceptance

**25.** Which of the following risks is best described as the expression of (the likelihood of occurrence after controls are applied) × (expected loss)?

**C.** Residual risk

**26.** Which of the following risk types best describes an example of insurance?

**B.** Risk transfer

**27.** Which of the following risk types relates to negative public opinion?

**C.** Reputation risk

**28.** Compliance risk as it relates to federal and state regulations can never be _____.

**B.** Transferred

**29.** Which of the following statements best describes organizations that are required to comply with multiple federal and state regulations?

**C.** They must ensure that their information security program includes all applicable requirements.

**30.** Which of the following terms best describes "duty of care" as applied to corporate directors and executive officers?

**A.** It's a legal obligation.

 

# CHAPTER 5
# ASSET MANAGEMENT

## KEY TERMS

 

**Confidential information:** Information meant to be kept secret and limited to only a small circle of authorized individuals.

**Declassification:** Involves reducing the level of classification of an information item. Note that in the military, declassifying does not mean to "lower the classification level." It always means to "remove the classification level."

**Information asset:** A definable piece of information that is recognized as having value to an organization.

**Information systems:** Hardware and software solutions that provide a way and a place to process, store, transmit, and communicate information.

**Non-public personal information (NPPI):** Information considered to be personal in nature, subject to public availability, and if disclosed is an invasion of privacy.

**Policy:** A set of rules combined to create a management framework that dictates how an organization will function.

**Public information:** Information that can be disclosed to the public without any adverse repercussions for a company.

**Reclassification:** Involves changing the classification level of an information item, either up or down.

# TEACHING NOTES

I. Information Assets and Systems

**Teaching Tips:** Emphasize that information assets are information used by a company (regardless of size) to fulfill its mission or goal. Many information assets are used to support internal operations, such as payroll.

Who Is Responsible for Information Assets?

**Teaching Tips:** Remind students that the information asset owner is liable and responsible for protecting the information and the business results derived from using that information (as opposed to merely updating the information). Every information asset needs an owner, but it is not always apparent or obvious who should be or is willing to assume the responsibility of ownership.

Responsibility for information security is often delegated to information custodians, whereas the information security officer ensures that appropriate controls are applied consistently throughout the organization.

II. Information Classification

**Teaching Tip:** Mention that the objective of an information classification system is to differentiate data types. Classification systems are used in government, military, and private sector and all these systems differ. Ask students to identify how information is classified by federal agencies, by military, and by private organizations.

Information may also need to be protected due to its intelligence value to others. Note to students that hacking begins with the process of gathering clues from information that is readily available.

III. Labeling and Handling Standards

 

**Teaching Tip:** Discuss that labels are used to identify the data classification. Explain that labels can be in many different forms, such as, electronic, print, audio, and visual. Ask students to find an example of each type of label and share it with the class. Have students develop a data handling standards matrix for a college. Student can use the sample matrix on pg. 137, Table 5.1 as a guide.

IV. Information Systems Inventory

**Teaching Tips:** The critical decision is choosing what attributes and characteristics of the information asset you want to record. Remember that over time your inventory may have multiple purposes.

# PROJECTS/EXERCISES

I. **Discussion Questions**

A. Discussion Question 1

Many organizations do not have an up-to-date inventory of information systems. What are the benefits of such an inventory?

Answer: Students' answers will vary. Identified benefits of an information systems inventory may include consolidation and/or merger of redundant systems (or information); improved business impact and disaster recovery planning insurance coverage; business valuation; and enhanced criticality and risk analysis.

B. Discussion Question 2

What sorts of routine, seemingly unimportant information would help you learn about or break into another company's network?

Answer: Student answers will vary. Possible answers include policy and procedure manuals, telephone and email lists, corporate web pages, network maps or other information (for example, server names), and discarded paperwork.

# CHAPTER REVIEW/ANSWERS TO TEST YOUR SKILLS

**MULTIPLE CHOICE**

**1.** Which of the following terms best describes a definable piece of information, stored in any manner that is recognized as having value to the organization?

**B.** Information asset

**2.** Information systems _____, _____, and _____ information.

**C.** Store, process, and transmit

**3.** Information owners are responsible for which of the following tasks?

**A.** Classifying information

**4.** Which of the following roles is responsible for implementing and maintaining security controls?

**D.** Information custodian

**5.** FIPS-199 requires that federal government information and information systems be classified as _____.

**A.** Low security

**B.** Moderate security

**C.** High security

**6.** Information classification systems are used in which of the following organizations?

**D.** All the above

**7.** FIPS requires that information be evaluated for _____requirements with respect to the impact of unauthorized disclosure as well as the use of the information.

**C.** Confidentiality

**8.** Which of the following National Security classifications requires the most protection?

**B.** Top Secret

**9.** Which of the following National Security classifications requires the least protection?

**B.** Unclassified

**10.** The Freedom of Information Act (FOIA) allows anyone access to which of the following?

**D.** Access to any records from federal agencies unless the documents can be officially declared exempt

**11.** Which of the following terms best describes the CIA attribute associated with the modification of information?

**B.** Integrity

**12.** Is it mandatory for all private businesses to classify information?

**D.** No.

**13.** Which of the following is not a criterion for classifying information?

**B.** The information has no value to the organization.

**14.** Data that is considered to be personal in nature and, if disclosed, is an invasion of privacy and a compromise of security is known as which of the following?

**C.** Nonpublic personal information

**15.** Most organizations restrict access to protected, confidential, and internal use data to which of the following roles within the organization?

 

**C.** Users who have a “need to know”

**16.** Labeling is the vehicle for communicating classification levels to which of the following roles within the organization?

**D.** All the above

**17.** Which of the following terms best describes rules for how to store, retain, and destroy data based on classification?

**A.** Handling standards

**18.** Which of the following terms best describes the process of removing restricted classification levels?

**A.** Declassification

**19.** Which of the following terms best describes the process of upgrading or changing classification levels?

**C.** Reclassification

**20.** The impact of destruction and/or permanent loss of information is used to determine which of the following safeguards?

**B.** Availability

**21.** Which of the following terms best describes an example of a hardware asset?

**A.** Server

**22.** Which of the following statements best describes a MAC address?

**C.** A MAC address is a unique hardware identifier.

**23.** 10.1.45.245 is an example of which of the following?

**C.** An IP address

**24.** Code and databases are examples of which of the following?

**A.** Software assets

**25.** Which of the following terms best describes the act of classifying information based on an original classification decision already made by an authorized original classification authority?

**B.** Derivative classification

**26.** Which of the following types of information would not be considered NPPI?

**D.** Home address

**27.** In keeping with best practices and regulatory expectations, legally protected data that is stored on mobile devices should be _____.

**B.** Encrypted

 

**28.** Which of the following statements best describes how written documents that contain NPPI should be handled?

**D.** All the above.

**29.** Which of the following address types represents a device location on a network?

**C.** A logical address

**30.** Which of the following statements is true?

**C.** Small businesses need to classify data because small businesses are responsible for protecting NPPI, employee data, and company data.

# CHAPTER 6
# HUMAN RESOURCES SECURITY

## KEY TERMS

**Confidentiality or nondisclosure agreements:** Contracts entered into by the employee and the organization in which the parties agree that certain type of information remain confidential.

**Security clearance investigation:** An inquiry into an individual's loyalty, character, trustworthiness, and reliability to ensure that he is eligible for access to national security-related information.

**Security incident:** Any adverse event whereby confidentiality, integrity, and/or availability of an information system (or information itself) is threatened.

**User provisioning:** The process of creating user accounts and group memberships, providing company identification, assigning access rights and permissions, as well as access devices, such as smart cards and tokens.

## TEACHING NOTES

I. The employee lifecycle

**Teaching Tips:** The employee lifecycle model represents the stages in the employee's career. Common stages include recruitment, onboarding, user provisioning, orientation, career development, termination. Have students identify the various processes occurring in each step.

Job Postings

**Teaching Tips:** Job postings are one of the sources that intruders often look to use for information that can be used in social engineering attacks and provide a path to more in-depth knowledge.

Ask students how information regarding specific systems, software, security features, or access controls in a job description can be misused.

The Interview

**Teaching Tips:** Interviewers often reveal much more than they should to early-stage job candidates. Have students think back to previous interviews and relate relevant stories.

II. The Importance of Employee Agreements

**Teaching Tips:** Ask students what should be included in an acceptable use agreement. Have students discuss the expectation of privacy at the workplace. Ask students to share their opinion on whether employers should monitor employees' Facebook and other social networking profiles.

III. The Importance of Security Education and Training

**Teaching Tips:** Have students discuss why security education and training is important. Have students identify the type of training that should be included in a security education program and how often these programs should be conducted. Ask students to identify current awareness programs and program goals.

# PROJECTS/EXERCISES

I. **Discussion Questions**

A. Discussion Question 1

Why does the U.S. Government require both a level of security clearance (at least equal to the classification of the information) and an appropriate "need to know" the information before information is released to an individual?

Answer: Student answers will vary. Merely having a certain level of security clearance does not authorize an individual to access all information so classified. Information must be closely held to be protected, so requiring both an equivalent security clearance and an authorized "need to know" restricts access appropriately. Background checks are more stringent for higher security clearance levels.

B. Discussion Question 2

What should be included in an acceptable use agreement?

Answer: Student answers will vary, but at a minimum the following components should be included in an acceptable use agreement: introduction, data classifications, applicable policy statement, handling standards, contacts, violations section, and acknowledgment.

 

## CHAPTER REVIEW/ANSWERS TO TEST YOUR SKILLS

### MULTIPLE CHOICE

**1.** Which of the following statements best describes the employee lifecycle?

**D.** The employee lifecycle spans recruitment to termination.

**2.** At which of the following phases of the hiring process should personnel security practices begin?

**C.** Recruitment

**3.** A published job description for a web designer should not include which of the following?

**C.** Specifics about the web development tool the company is using

**4.** Data submitted by potential candidates must be _____.

**A.** Protected as required by applicable law and organizational policy

**5.** During the course of an interview, a job candidate should be given a tour of which of the following locations?

**B.** Public areas only (unless otherwise authorized)

**6.** Which of the following facts is an interviewer permitted to reveal to a job candidate?

**D.** The duties and responsibilities of the position

**7.** Which of the following statements best describes the reason for conducting background checks?

**A.** To verify the truthfulness, reliability, and trustworthiness of the applicant

**8.** Which of the following statements best describes the background check criteria?

**C.** Criteria should be specific to the job for which an applicant is applying.

**9.** Social media profiles often include gender, race, and religious affiliation. Which of the following statements best describes how this information should be used in the hiring process?

**B.** Gender, race, and religious affiliation cannot legally be used in making hiring decisions.

**10.** Under the Fair Credit Reporting Act (FCRA), which of the following statements is true?

**B.** Employers must get the candidate's consent to request a credit report.

**11.** Candidate and employee NPPI must be protected. NPPI does not include which of the following?

**C.** Published telephone number

 

**12.** Which of the following statements best describes the purpose of completing the Department of Homeland Security/U.S. Citizenship and Immigration Services Form I-9 and providing supporting documentation?

**A.** The purpose is to establish identity and employment authorization.

**13.** The permissions and access rights a user is granted should match his role and responsibilities. Who is responsible for defining to whom access should be granted?

**B.** The information owner

**14.** Network administrators and help desk personnel often have elevated privileges. They are examples of which of the following roles?

**B.** The information custodians

**15.** Which of the following statements is *not* true of confidentiality agreements?

**D.** Confidentiality agreements should be required only of top-level executives.

**16.** Which of the following elements would you expect to find in an acceptable use agreement?

**A.** Handling standards

**17.** Which of the following statements best describes when acceptable use agreements should be reviewed, updated, and distributed?

**B.** Acceptable use agreements should be reviewed, updated, and distributed annually.

**18.** Which of the following terms best describes the SETA acronym?

**B.** Security Education Training Awareness

**19.** Posters are placed throughout the workplace reminding users to log off when leaving their workstations unattended. This is an example of which of the following programs?

**C.** A security awareness program

**20.** A network engineer attends a 1-week hands-on course on firewall configuration and maintenance. This is an example of which of the following programs?

**B.** A security training program

**21.** The Board of Directors has a presentation on the latest trends in security management. This is an example of which of the following programs?

**A.** A security education program

**22.** Companies have the legal right to perform which of the following activities?

**A.** Monitor user Internet access from the workplace.

**23.** Sanctions for policy violations should be included in which of the following documents?

 

**D.** All the above

**24.** Studies often cite _____ as the weakest link in information security.

**B.** People

**25.** Which of the following terms best describes the impact of security education?

**A.** Long-term

**26.** Which of the following privacy regulations stipulates that schools must have written permission to release any information from a student's education record?

**D.** FERPA

**27.** Which of the following regulations specifically stipulates that employees should be trained on password management?

**B.** HIPAA

**28.** Best practices dictate that employment applications should *not* ask prospective employees to provide which of the following information?

**C.** Social Security number

**29.** After a new employee's retention period has expired, completed paper employment applications should be _____.

**A.** Cross-cut shredded

**30.** Intruders might find job posting information useful for which of the following attacks?

**B.** A social engineering attack

 