CHAPTER 1: POLICY DEFINED

Multiple Choice:

1. Which of the following is NOT a state in which information exists?

A. stored

B. processed

C. factored

D. transmitted

Answer: C **Reference:** Defining Policy **Difficulty:** easy

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

Answer: A **Reference:** Enforcing Technological Policies **Difficulty:** moderate

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

Answer: B **Reference:** Understanding the Psychology of Policy **Difficulty:** easy

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

Answer: B **Reference:** Consistency in Services, Products, and Corporate Culture **Difficulty:** moderate

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

Answer: A **Reference:** Organizational Culture Comes from the Top **Difficulty:** moderate

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

Answer: D **Reference:** Changes in the Environment **Difficulty:** easy

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

Answer: A **Reference:** Understanding the Psychology of Policy **Difficulty:** moderate

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

Answer: C **Reference:** Introducing Policies to the Organization **Difficulty:** easy

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

Answer: B **Reference:** Getting Approval **Difficulty:** moderate

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

Answer: A **Reference:** Complying with Government Policies **Difficulty:** moderate

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

Answer: C **Reference:** Enforcing Behavioral Policies **Difficulty:** moderate

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

Answer: D **Reference:** Organizational Culture Comes from the Top **Difficulty:** easy

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

Answer: D **Reference:** Reinforcement Through Good Communication **Difficulty:** moderate

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

Answer: A **Reference:** Responding to Environmental Changes **Difficulty:** moderate

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

Answer: C **Reference:** The Bible as Ancient Policy **Difficulty:** moderate

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

Answer: B **Reference:** The U.S. Constitution as a Policy Revolution **Difficulty:** moderate

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

Answer: D **Reference:** The U.S. Constitution as a Policy Revolution **Difficulty:** moderate

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

Answer: B **Reference:** The Bible as Ancient Policy **Difficulty:** moderate

Fill in the Blank:

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

Answer: gap **Reference:** Involving Those Who Know What Is Possible **Difficulty:** moderate

20. An organization which does not enforce policy is said to have ____________ policies.

Answer: paper only **Reference:** Enforcing Behavioral Policies **Difficulty:** moderate

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

Answer: Board of Directors **Reference:** Involving Those Who Know What Is Possible **Difficulty:** easy

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

Answer: disclosure **Reference:** Complying with Government Policies **Difficulty:** moderate

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

Answer: amendments **Reference:** The U.S. Constitution as a Policy Revolution **Difficulty:** easy

Matching:

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

I.	Board of Directors	A. Ensure that information security controls are functioning as intended
II.	Information Owner	B. Approve written information security policies
III.	Data Custodian	C. Establish the controls that provide information security
IV.	ISO	D. Process and store information
V.	Internal Auditor	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	A. Policy adopted by society through legislative means to govern its people
II.	Law	B. Civil or criminal; imposed for violations
III.	Policy Area	C. A general topic, which relates to specific behavior and expectations
IV.	Penalty	D. Standards for public and private education
V.	Education Policy	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