1. Policies define which of the following?
A. Rules
B. Expectations
C. Patterns of behavior
D. All of the above

2. Without policy, human beings would live in a state of _____.
A. chaos
B. bliss
C. harmony
D. laziness

3. A guiding principle is best described as which of the following?
A. A financial target
B. A fundamental philosophy or belief
C. A regulatory requirement
D. A person in charge

4. Which of the following best describes corporate culture?
A. Shared attitudes, values, and goals
B. Multiculturalism
C. A requirement to all act the same
D. A religion

5. Which of the following is a true statement?
A. Corporate culture is the same as policy.
B. Guiding principles set the tone for a corporate culture.
C. All corporate cultures are positive.
D. Guiding principles should be kept secret.

6. Which of the following best describes the role of policy?
A. To codify guiding principles
B. To shape behavior
C. To serve as a roadmap
D. All of the above

7. An information security policy is a directive that defines which of the following?
A. How employees should do their jobs
B. How to pass an annual audit
C. How an organization protects information assets and systems
D. How much security insurance a company should have

8. Which of the following is not an example of an information asset?
A. Customer financial records
B. Marketing plan
C. Patient medical history
D. Building graffiti

9. What are the seven characteristics of a successful policy?
A. Endorsed, relevant, realistic, cost-effective, adaptable, enforceable, inclusive
B. Endorsed, relevant, realistic, attainable, adaptable, enforceable, inclusive
C. Endorsed, relevant, realistic, technical, adaptable, enforceable, inclusive
D. Endorsed, relevant, realistic, legal, adaptable, enforceable, inclusive

10. A policy that has been endorsed has the support of which of the following?
A. Customers
B. Creditors
C. The union
D. Management

11. Who should always be exempt from policy requirements?
A. Employees
B. Executives
C. No one
D. Salespeople

12. "Attainable" means that the policy _____.
A. can be successfully implemented
B. is expensive
C. only applies to suppliers
D. must be modified annually

13. Which of the following statements is always true?
A. Policies stifle innovation.
B. Policies make innovation more expensive.
C. Policies should be adaptable.
D. Effective policies never change.

14. If a policy is violated and there is no consequence, the policy is considered to be which of the following?
A. Meaningless
B. Inclusive
C. Legal
D. Expired

15. Who must approve the retirement of a policy?
A. A compliance officer
B. An auditor
C. Executive management or the Board of Directors
D. Legal counsel

16. Which of the following sectors is not considered part of the "critical infrastructure"?
A. Public health
B. Commerce
C. Banking
D. Chemical industry

17. Which term best describes government intervention with the purpose of causing a specific set of actions?
A. Deregulation
B. Politics
C. Regulation
D. Amendments

18. The objectives of GLBA and HIPAA, respectively, are to protect _____.
A. financial and medical records
B. financial and credit card records
C. medical and student records
D. judicial and medical records

19. Which of the following states was the first to enact consumer breach notification?
A. Kentucky
B. Colorado
C. Connecticut
D. California

20. In 2010, Massachusetts became the first state in the nation to require _____.
A. minimum standards for the protection of personally identifiable information of non-residents
B. minimum standards for the protection of personally identifiable information of Massachusetts residents
C. maximum standards for the protection of personally identifiable information of Massachusetts residents
D. consumer notification of a breach

21. Which of the following terms best describes the process of developing, publishing, adopting, and reviewing a policy?
A. Policy two-step
B. Policy aging
C. Policy retirement
D. Policy lifecycle

22. Who should be involved in the process of developing policies?
A. Only upper-management-level executives
B. Only part-time employees
C. Personnel throughout the company
D. Only outside, third-party consultants

23. Which of the following does *not* happen in the policy development phase?
A. Planning
B. Enforcement
C. Authorization
D. Approval

24. Which of the following occurs in the policy publication phase?
A. Communication
B. Policy dissemination
C. Education
D. All of the above

25. Normative integration is the goal of the adoption phase. This means _____.
A. A here are no exceptions to the policy.
B. The policy passes the stress test.
C. The policy becomes expected behavior, all others being deviant.
D. The policy costs little to implement.

26. How often should policies be reviewed?
A. Never
B. Only when there is a significant change
C. Annually
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
B. Winning a compliance award
C. Voting to authorize a policy
D. None of the above

28. Which of the following phrases best describes the philosophy of “honoring the public trust”?
A. Being respectful of law enforcement
B. Contributing to political campaigns
C. Being a careful steward of information in your care
D. Visiting government monuments

29. Who should authorize policies?
A. Directors or executive management
B. Operational managers
C. Employees
D. Legal counsel

30. Which of the following statements is *not* an objective of information security?
A. To protect information and information systems from intentional misuse
B. To protect information and information systems from compromise
C. To protect information and information systems from destruction
D. To protect information and information systems from authorized users

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.

CH2
1. The policy hierarchy is the relationships between which of the following?
A. Guiding principles, regulations, laws, and procedures
B. Guiding principles, standards, guidelines, and procedures
C. Guiding principles, instructions, guidelines, and programs
D. None of the above

2. Which of the following statements best describes the purpose of a standard?
A. To state the beliefs of an organization
B. To reflect the guiding principles
C. To dictate mandatory requirements
D. To make suggestions

3. Which of the following statements best describes the purpose of a guideline?
A. To state the beliefs of an organization
B. To reflect the guiding principles
C. To dictate mandatory requirements
D. To make suggestions

4. Which of the following statements best describes the purpose of a baseline?
A. To measure compliance
B. To ensure uniformity across a similar set of devices
C. To ensure uniformity across different devices
D. To make suggestions

5. Simple Step, Hierarchical, Graphic, and Flowchart are examples of which of the following formats?
A. Policy
B. Program
C. Procedure
D. Standard

6. Which of the following terms best describes instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain timeframe, usually with defined stages and with designated resources?
A. Plan
B. Policy
C. Procedure
D. Package

7. Which of the following statements best describes a disadvantage to using the singular policy format?
A. The policy can be short.
B. The policy can be targeted.
C. You may end up with too many policies to maintain.
D. The policy can easily be updated.

8. Which of the following statements best describes a disadvantage to using the consolidated policy format?
A. Consistent language is used throughout the document.
B. Only one policy document must be maintained.
C. The format must include a composite management statement.
D. The potential size of the document.

9. Policies, standards, guidelines, and procedures should all be in the same document.
A. True
B. False
C. Only if the company is multinational
D. Only if the documents have the same author

10. Version control is the management of changes to a document and should include which of the following elements?
A. Version or revision number
B. Date of authorization
C. Change description
D. All of the above

11. Which of the following is not a policy introduction objective?
A. To convey the importance of understanding and adhering to the policy
B. To provide explicit instructions on how to comply with the policy
C. To explain the exemption process as well as the consequence of non-compliance
D. To thank the reader and to reinforce the authority of the policy

12. The name of the policy, policy number, and overview belong in which of the following sections?
A. Introduction
B. Policy Heading
C. Policy Goals and Objectives
D. Policy Statement

13. The aim or intent of a policy is stated in the _____.
A. introduction
B. policy heading
C. policy goals and objectives
D. policy statement

14. Which of the following statements is true?
A. A security policy should only include one objective.
B. A security policy should not include any exceptions.
C. A security policy should not include a glossary.
D. A security policy should not list all step-by-step measures that need to be taken.

15. The _____ contains the rules that must be followed.
A. policy heading
B. policy statement
C. policy enforcement clause
D. policy goals and objectives

16. A policy should be considered _____.
A. mandatory
B. discretionary
C. situational
D. optional

17. Which of the following best describes policy definitions?
A. A glossary of terms used
B. A detailed list of the possible penalties associated with breaking rules set forth in the policy
C. A list of all the members of the security policy creation team
D. None of the above

18. The _____ contains the penalties that would apply if a portion of the security policy were to be ignored by an employee.
A. policy heading
B. policy statement
C. policy enforcement clause
D. policy statement of authority

19. What component of a security policy does the following phrase belong to?
"Wireless networks are allowed only if they are separate and distinct from the corporate network."
A. Introduction
B. Administrative notation
C. The policy heading
D. The policy statement

20. There may be situations where it is not possible to comply with a policy directive.
Where should the exemption or waiver process be explained?
A. Introduction
B. The policy statement
C. The policy enforcement clause
D. The policy exceptions

21. The name of the person/group (for example, executive committee) that authorized the policy should be included in _____.
A. the version control table or the policy statement
B. the heading or the policy statement
C. the policy statement or the policy exceptions
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
B. be as vague as possible
C. reference another, dedicated document
D. None of the above

23. If supporting documentation would be of use to the reader, it should be _____.
A. included in full in the policy document
B. ignored because supporting documentation does not belong in a policy document
C. listed in either the Policy Heading or Administrative Notation section
D. included in a policy appendix

24. When writing a policy, standard, guideline, or procedure, you should use language that is _____.
A. technical
B. clear and concise
C. legalese
D. complex

25. Readers prefer "plain language" because it _____.
A. helps them locate pertinent information
B. helps them understand the information
C. saves time
D. All of the above

26. Which of the following is not a characteristic of plain language?
A. Short sentences
B. Using active voice
C. Technical jargon
D. Seven or fewer lines per paragraph

27. Which of the following terms is best to use when indicating a mandatory requirement?
A. must
B. shall
C. should not
D. may not

28. A company that uses the term "employees" to refer to workers who are on the company payroll should refer to them throughout their policies as _____.
A. workforce members
B. employees
C. hired hands
D. workers

29. "The ball was thrown by Sam to Sally" is a passive sentence. Which of the following sentences represents an active version of this sentence?
A. The ball was thrown to Sally by Sam.
B. Sally caught the ball.
C. Sam threw the ball to Sally.
D. The ball was thrown by Sam to Sally, who caught it.

30. Even the best-written policy will fail if which of the following is true?
A. The policy is too long.
B. The policy is mandated by the government.
C. The policy doesn't have the support of management.
D. All of the above.

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

CH3

1. Which of the following are the three principles in the CIA triad?
A. Confidence, integration, availability
B. Consistency, integrity, authentication
C. Confidentiality, integrity, availability
D. Confidentiality, integrity, awareness

2. Which of the following is an example of acting upon the goal of integrity?
A. Ensuing that only authorized users can access data
B. Ensuring that systems have 99.9% uptime
C. Ensuring that all modifications go through a change-control process
D. Ensuring that changes can be traced back to the editor

3. Which of the following is a control that relates to availability?
A. Disaster recovery site
B. Firewall
C. Training
D. Encryption

4. Which of the following is an objective of confidentiality?
A. Protection from unauthorized access
B. Protection from manipulation
C. Protection from denial of service
D. Protection from authorized access

5. As it pertains to information security, assurance is _____.
A. the process of tracing actions to their source
B. the processes, policies, and controls used to develop confidence that security measures are working as intended
C. the positive identification of the person or system seeking access to secured information or systems
D. the logging of access and usage of information resources

6. Which of the following terms best describes the granting of users and systems a predetermined level of access to information resources?
A. Availability
B. Accountability
C. Assurance
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
B. Loss of confidentiality due to unauthorized access
C. Loss of personnel due to accident
D. Loss of reputation from unauthorized event

8. Which of the following terms best describes the logging of access and usage of information resources?
A. Accountability
B. Acceptance
C. Accounting
D. Actuality

9. Which of the following combination of terms best describes the Five A's of information security?
A. Awareness, acceptance, availability, accountability, authentication
B. Awareness, acceptance, authority, authentication, availability
C. Accountability, assurance, authorization, authentication, accounting
D. Acceptance, authentication, availability, assurance, accounting

10. An information owner is responsible for _____.
A. maintaining the systems that store, process, and transmit information
B. protecting the information and the business results derived from use of that information
C. protecting the people and processes used to access digital information
D. none of the above

11. Which of the following terms best describes ISO?
A. Internal Standards Organization
B. International Organization for Standardization
C. International Standards Organization
D. Internal Organization of Systemization

12. Which of the following statements best describes opportunistic crime?
A. Crime that is well-planned
B. Crime that is targeted
C. Crime that takes advantage of an identified weakness
D. Crime that is quick and easy

13. Which of the following terms best describes the motivation for hactivism?
A. Financial
B. Political
C. Personal
E. Fun

14. The greater the criminal work factor, the _____
A. more time it takes
B. more profitable the crime is
C. better chance of success
D. less chance of getting caught

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?
A. Man-in-the-middle
B. Data breach
C. Denial of service
D. SQL injection

16. Information custodians are responsible for _____
A. writing policy
B. classifying data
C. approving budgets
E. implementing safeguards

17. The National Institute of Standards and Technology (NIST) is a(n) _____
A. international organization
B. privately funded organization
C. U.S. government agency
D. European Union agency

18. The Internal Organization for Standardization (ISO) is _____
A. a nongovernmental organization
B. an international organization
C. headquartered in Geneva
D. all of the above

19. The current ISO family of standards that relates to information security is _____.
A. BS 7799:1995
B. ISO 17799:2006
C. ISO/IEC 27000
D. None of the above

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?
A. Security policy
B. Access control
C. Compliance
D. Risk assessment

21. Which of the following terms best describes the security domain that relates to how data is classified and valued?
A. Security policy
B. Asset management
C. Compliance
D. Access control

22. Which of the following terms best describes the security domain that includes HVAC, fire suppression, and secure offices?
A. Operations
B. Communications
C. Risk assessment
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
B. Compliance
C. Incident management
D. Business continuity

24. The primary objective of the _____ domain is to ensure conformance with GLBA, HIPAA, PCI/DSS, FERPA, and FISMA.
A. Security Policy
B. Compliance
C. Access Control
D. Contract and Regulatory

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

B. Operations and Communications
C. Incident Management
D. Business Continuity Management

26. Which of the following terms best describes a synonym for business continuity?
A. Authorization
B. Authentication
C. Availability
D. Accountability

27. The _____ can be held legally responsible for the safeguarding of legally protected information.
A. information user
B. information owner
C. information custodian
D. information author

28. Personnel screening, acceptable use, confidentiality agreements, and training are controls that relate to the _____ domain.
A. Operations and Communications
B. Security Policy
C. Human Resources
D. Legal and Compliance

29. Defining organizational roles, responsibilities, and authority relate to the _____ domain.
A. Operations and Communications
B. Security Policy
C. Governance
D. Legal and Compliance

30. Which of the following security objectives is most important to an organization?
A. Confidentiality
B. Integrity
C. Availability
D. The answer may vary from organization to organization.

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.

CH4
1. When an information security program is said to be "strategically aligned," this indicates that _____.
A. It supports business objectives
B. It adds value
C. It maintains compliance with regulatory requirements
D. All of the above

2. How often should information security policies be reviewed?
A. Once a year
B. Only when a change needs to be made
C. At a minimum, once a year and whenever there is a change trigger
D. Only as required by law

3. Information security policies should be authorized by _____.
A. the Board of Directors (or equivalent)
B. business unit managers
C. legal counsel
D. stockholders

4. Which of the following statements best describes policies?
A. Policies are the implementation of specifications.
B. Policies are suggested actions or recommendations.
C. Policies are instructions.
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?
A. Sections of the comprehensive policy may not be applicable to all employees.
B. The comprehensive policy may include unknown acronyms.
C. The comprehensive document may contain confidential information.
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.
B. Covered entities must use federally mandated technology.
C. Covered entities must self-report compliance.
D. Covered entities must notify law enforcement if there is a policy violation.

7. Organizations that choose to adopt the ISO 27002:2103 framework must _____.
A. use every policy, standard, and guideline recommended
B. create policies for every security domain
C. evaluate the applicability and customize as appropriate
D. register with the ISO

8. Evidence-based techniques used by information security auditors include which of the following elements?
A. Structured interviews, observation, financial analysis, and documentation sampling
B. Structured interviews, observation, review of practices, and documentation sampling
C. Structured interviews, customer service surveys, review of practices, and documentation sampling
D. Casual conversations, observation, review of practices, and documentation sampling

9. Which of the following statements best describes independence in the context of auditing?
A. The auditor is not an employee of the company.
B. The auditor is certified to conduct audits.
C. The auditor is not responsible for, benefited from, or in any way influenced by the audit target.
D. Each auditor presents his or her own opinion.

10. Which of the following states is *not* included in a CMM?
A. Average
B. Optimized
C. Ad hoc
D. Managed

11. Which of the following activities is not considered a governance activity?
A. Managing
B. Influencing
C. Evaluating
D. Purchasing

12. To avoid conflict of interest, the CISO could report to which of the following individuals?
A. The Chief Information Officer (CIO)
B. The Chief Technology Officer (CTO)
C. The Chief Financial Officer (CFO)
D. The Chief Compliance Officer (CCO)

13. Which of the following statements best describes the role of the Information Security Steering Committee?
A. The committee authorizes policy.
B. The committee serves in an advisory capacity.
C. The committee approves the InfoSec budget.
D. None of the above.

14. Defining protection requirements is the responsibility of _____.
A. the ISO
B. the data custodian
C. data owners
D. the Compliance Officer

15. Designating an individual or team to coordinate or manage information security is required by _____.
A. GLBA
B. MA CMR 17 301
C. PCI DSS
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?
A. Threat
B. Risk
C. Vulnerability
D. Impact

17. Inherent risk is the state before _____.
A. an assessment has been conducted
B. security measures have been implemented
C. the risk has been accepted
D. None of the above

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?
A. Risk
B. Threat source
C. Threat
D. Vulnerability

19. Which of the following terms best describes a disgruntled employee with intent to do harm?
A. Risk
B. Threat source
C. Threat
D. Vulnerability

20. Which if the following activities is *not* considered an element of risk management?
A. The process of determining an acceptable level of risk
B. Assessing the current level of risk for a given situation
C. Accepting the risk
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 _____.
A. risk acceptance
B. risk tolerance
C. risk mitigation
D. risk avoidance

22. Which of the following statements best describes a vulnerability?
A. A vulnerability is a weakness that could be exploited by a threat source.
B. A vulnerability is a weakness that can never be fixed.
C. A vulnerability is a weakness that can only be identified by testing.
D. A vulnerability is a weakness that must be addressed regardless of the cost.

23. A control is a security measure that is designed to _____ a threat source.
A. detect
B. deter
C. prevent
D. All of the above

24. Which of the following is not a risk-mitigation action?
A. Risk acceptance
B. Risk sharing or transference
C. Risk reduction
D. Risk avoidance

25. Which of the following risks is best described as the expression of (the likelihood of occurrence after controls are applied) × (expected loss)?
A. Inherent risk
B. Expected risk
C. Residual risk
D. Accepted risk

26. Which of the following risk types best describes an example of insurance?
A. Risk avoidance
B. Risk transfer
C. Risk acknowledgement
D. Risk acceptance

27. Which of the following risk types relates to negative public opinion?
A. Operational risk
B. Financial risk
C. Reputation risk
D. Strategic risk

28. Compliance risk as it relates to federal and state regulations can never be _____.
A. avoided
B. transferred
C. accepted
D. None of the above

29. Which of the following statements best describes organizations that are required to comply with multiple federal and state regulations?
A. They must have different policies for each regulation.
B. They must have multiple ISOs.
C. They must ensure that their information security program includes all applicable requirements.
D. They must choose the one regulation that takes precedence.

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.
B. It's an outdated requirement.
C. It's ignored by most organizations.
D. It's a factor only when there is a loss greater than $1,000.

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.

CH5

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?
A. NPPI
B. Information asset
C. Information system
D. Classified data

2. Information systems _____, _____, and _____ information.
A. create, modify, and delete
B. classify, reclassify, and declassify
C. store, process, and transmit
D. use, label, and handle

3. Information owners are responsible for which of the following tasks?
A. Classifying information
B. Maintaining information
C. Using information
D. Registering information

4. Which of the following roles is responsible for implementing and maintaining security controls?
A. Information owner
B. Information vendor
C. Information user
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
D. None of the above

6. Information classification systems are used in which of the following organizations?
A. Government
B. Military
C. Financial institutions
D. All of 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.
A. integrity
B. availability
C. confidentiality
D. secrecy

8. Which of the following National Security classifications requires the most protection?
A. Secret
B. Top Secret
C. Confidential
D. Unclassified

9. Which of the following National Security classifications requires the least protection?
A. Secret
B. Unclassified
C. Confidential
D. Sensitive But Unclassified (SBU)

10. The Freedom of Information Act (FOIA) allows anyone access to which of the following?
A. Access to all government information just by asking
B. Access to all classified documents
C. Access to classified documents on a "need to know" basis
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?
A. Classified
B. Integrity
C. Availability
D. Intelligence

12. Is it mandatory for all private businesses to classify information?
A. Yes.
B. Yes, but only if they want to pay less taxes.
C. Yes, but only if they do business with the government.
D. No.

13. Which of the following is not a criterion for classifying information?
A. The information is not intended for the public domain.
B. The information has no value to the organization.
C. The information needs to be protected from those outside of the organization.
D. The information is subject to government regulations.

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?
A. Non-personal public information
B. Non-private personal information
C. Non-public personal information
D. None of the above

15. Most organizations restrict access to protected, confidential, and internal-use data to which of the following roles within the organization?
A. Executives
B. Information owners
C. Users who have a "need to know"
D. Vendors

16. Labeling is the vehicle for communicating classification levels to which of the following roles within the organization?
A. Employees
B. Information custodians
C. Contractors
D. All of 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
B. Classification procedures
C. Use policies
D. Material guidelines

18. Which of the following terms best describes the process of removing restricted classification levels?
A. Declassification
B. Classification
C. Reclassification
D. Negative classification

19. Which of the following terms best describes the process of upgrading or changing classification levels?
A. Declassification
B. Classification
C. Reclassification
D. Negative classification

20. The impact of destruction and/or permanent loss of information is used to determine which of the following safeguards?
A. Authorization
B. Availability
C. Authentication
D. Accounting

21. Which of the following terms best describes an example of a hardware asset?
A. Server
B. Database
C. Hammer
D. Radio waves

22. Which of the following statements best describes a MAC address?
A. A MAC address is a unique network address.
B. A MAC address is a unique host name.
C. A MAC address is a unique hardware identifier.
D. A MAC address is a unique alias.

23. 10.1.45.245 is an example of which of the following?
A. A MAC address
B. A host name
C. An IP address
D. An IP domain name

24. Code and databases are examples of which of the following?
A. Software assets
B. Proprietary information
C. Internal-use classification
D. Intellectual property (IP)

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?
A. Reclassification
B. Derivative classification
C. Declassification
D. Original classification

26. Which of the following types of information would not be considered NPPI?
A. Social security number
B. Date of birth
C. Debit card PIN
D. Home address

27. In keeping with best practices and regulatory expectations, legally protected data that is stored on mobile devices should be _____.
A. masked
B. encrypted
C. labeled
D. segregated

28. Which of the following statements best describes how written documents that contain NPPI should be handled?
A. Written documents that contain NPPI should be stored in locked areas or in a locked cabinet.
B. Written documents that contain NPPI should be destroyed by cross-cut shredding.
C. Written documents that contain NPPI should be subject to company retention policies.
D. All of the above.

29. Which of the following address types represents a device location on a network?
A. A physical address
B. A MAC address
C. A logical address
D. A static address

30. Which of the following statements is true?
A. Small businesses do *not* need to classify data because it is unusual for a small business to have NPPI.
B. Small businesses do *not* need to classify data because small businesses do not have regulatory obligations.
C. Small businesses need to classify data because small businesses are responsible for protecting NPPI, employee data, and company data.
D. Small businesses need to classify data because every organization is legally required to have a classification system.

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.

CH6
1. Which of the following statements best describes the employee lifecycle?
A. The employee lifecycle spans recruitment to career development.
B. The employee lifecycle spans onboarding to orientation.
C. The employee lifecycle spans user provision to termination.
D. The employee lifecycle spans recruitment to termination.

2. At which of the following phases of the hiring process should personnel security practices begin?
A. Interview
B. Offer
C. Recruitment
D. Orientation

3. A published job description for a web designer should not include which of the following?
A. Job title
B. Salary range
C. Specifics about the web development tool the company is using
D. Company location

4. Data submitted by potential candidates must be _____.
A. protected as required by applicable law and organizational policy
B. not protected unless the candidate is hired
C. stored only in paper form
D. publicly accessible

5. During the course of an interview, a job candidate should be given a tour of which of the following locations?
A. The entire facility
B. Public areas only (unless otherwise authorized)
C. The server room
D. The wiring closet

6. Which of the following facts is an interviewer permitted to reveal to a job candidate?
A. A detailed client list
B. The home phone numbers of senior management
C. The organization's security weaknesses
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
B. To find out if the applicant ever got in trouble in high school
C. To find out if the applicant has a significant other
D. To verify the applicant's hobbies, number of children, and type of house

8. Which of the following statements best describes the background check criteria?
A. Criteria should be the same for all prospective employees.
B. Criteria should differ according to gender or ethnicity.
C. Criteria should be specific to the job for which an applicant is applying.
D. None of the above.

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?
A. Gender, race, and religious affiliation can legally be used in making hiring decisions.
B. Gender, race, and religious affiliation cannot legally be used in making hiring decisions.
C. Gender, race, and religious affiliation are useful in making hiring decisions.
D. Gender, race, and religious affiliation listed in social media profiles should not be relied upon as they may be false.

10. Under the Fair Credit Reporting Act (FCRA), which of the following statements is true?
A. Employers cannot request a copy of an employee's credit report under any circumstances.
B. Employers must get the candidate's consent to request a credit report.
C. Employers cannot use credit information to deny a job.
D. Employers are required to conduct credit checks on all applicants.

11. Candidate and employee NPPI must be protected. NPPI does not include which of the following?
A. Social security number
B. Credit card number
C. Published telephone number
D. Driver's license number

12. Which of the following statements best describes the purpose of completing 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.
B. The purpose is to determine tax identification and withholding.
C. The purpose is to document educational achievements.
D. The purpose is to verify criminal records.

13. The permissions and access rights a user is granted should match their role and responsibilities. Who is responsible for defining to whom access should be granted?
A. The information user
B. The information owner
C. The information custodian
D. The information author

14. Network administrators and help desk personnel often have elevated privileges. They are examples of which of the following roles?
A. The information owners
B. The information custodians
C. The information authors
D. The information sellers

15. Which of the following statements is *not* true of confidentiality agreements?
A. Confidentiality/non-disclosure agreements are legal protection against unauthorized use of information.
B. Confidentiality/non-disclosure agreements are generally considered a condition of work.
C. Confidentiality/non-disclosure agreements are legally binding contracts.
D. Confidentiality agreements should only be required of top-level executives.

16. Which of the following elements would you expect to find in an acceptable use agreement?
A. Handling standards
B. A lunch and break schedule
C. A job description
D. An evacuation plan

17. Which of the following statements best describes when acceptable use agreements should be reviewed, updated, and distributed?
A. Acceptable use agreements should be reviewed, updated, and distributed only when there are organizational changes.
B. Acceptable use agreements should be reviewed, updated, and distributed annually.
C. Acceptable use agreements should be reviewed, updated, and distributed only during the merger and acquisition due diligence phase.
D. Acceptable use agreements should be reviewed, updated, and distributed at the discretion of senior management.

18. Which of the following terms best describes the SETA acronym?
A. Security Education Teaches Awareness
B. Security Education Training Awareness
C. Security Education Teaches Acceptance
D. Security Education Training Acceptance

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?
A. A security education program
B. A security training program
C. A security awareness program
D. None of the above

20. A network engineer attends a one-week hands-on course on firewall configuration and maintenance. This is an example of which of the following programs?
A. A security education program
B. A security training program
C. A security awareness program
D. None of the above

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
B. A security training program
C. A security awareness program
D. None of the above

22. Companies have the legal right to perform which of the following activities?
A. Monitor user Internet access from the workplace
B. Place cameras in locker rooms where employees change clothes
C. Conduct a search of an employee's home
D. None of the above

23. Sanctions for policy violations should be included in which of the following documents?
A. The employee handbook
B. A confidentiality/non-disclosure agreement
C. An acceptable use agreement
D. All of the above

24. Studies often cite _____ as the weakest link in information security.
A. policies
B. people
C. technology
D. regulations

25. Which of the following terms best describes the impact of security education?
A. Long-term
B. Short-term
C. Intermediate
D. Forever

26. Which of the following privacy regulations stipulates that schools must have written permission in order to release any information from a student's education record?
A. Sarbanes-Oxley Act (SOX)
B. HIPAA
C. Gramm-Leach-Bliley Act (GLBA)
D. FERPA

27. Which of the following regulations specifically stipulates that employees should be trained on password management?
A. FERPA
B. HIPAA
C. DPPA
D. FISMA

28. Best practices dictate that employment applications should *not* ask prospective employees to provide which of the following information?
A. Last grade completed
B. Current address
C. Social security number
D. Email address

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

A. cross-cut shredded
B. recycled
C. put in the trash
D. stored indefinitely

30. Intruders might find job posting information useful for which of the following attacks?
A. A distributed denial of service attack (DDoS) attack
B. A social engineering attack
C. A man-in-the-middle attack
D. An SQL injection attack

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