**Chapter 13 Review Questions**

1. Each of the following is a category of fire suppression systems except a \_\_\_\_\_\_\_\_\_.

a. clean agent system

b. dry chemical system

c. wet chemical system – PG507

d. water sprinkler system

2. Each of the following is required for a fire to occur except \_\_\_\_\_\_\_.

a. a spark to start the process

b. a type of fuel or combustible material

c. sufficient oxygen to sustain the combustion

d. a chemical reaction that is the fire itself – PG505

3. An electrical fire like that which would be found in a computer data center is known as what type of fire?

a. Class A

b. Class B

c. Class C – PG506

d. Class D

4. Van Eck phreaking is \_\_\_\_\_\_.

a. blocked by using shielded cabling

b. picking up electromagnetic fields generated by a computer system – PG508

c. reverse confidentiality

d. is always used with wireless networks

5. Plenums are .

a. no longer used today

b. the air-handling space above drop ceilings – PG509

c. required in all buildings with over six stories

d. never to be used for locating equipment

6. RAID\_\_\_\_\_ uses disk mirroring and is considered fault-tolerant.

a. Level 1 – PG497

b. Level 2

c. Level 3

d. Level 4

7. A standby server that exists only to take over for another server in the event of its failure is known as a(n) \_\_\_\_\_\_\_.

a. asymmetric server cluster – PG494

b. rollover server

c. failsafe server

d. symmetric server cluster

8. RAID is an abbreviation of

a. Redundant Array of IDE Drives

b. Resilient Architecture for Interdependent Discs

c. Redundant Array of Independent Drives – PG496

d. Resistant Architecture of Interrelated Data Storage

9. Which of the following is an example of a nested RAID?

a. Level 1-0

b. Level 0-1

c. Level 0+1 – PG497

d. Level 0/1

10. A(n) \_\_\_\_\_\_ is always running off its battery while the main power runs the battery charger.

a. offline UPS

b. backup UPS

c. online UPS – PG500

d. secure UPS

11. A \_\_\_\_ is essentially a duplicate of the production site and has all the equipment needed for an organization to continue running.

a. cold site

b. warm site

c. hot site – PG500-501

d. replicated site

12. A UPS can perform each of the following except \_\_\_\_.

a. prevent certain applications from launching that will consume too much power – PG500

b. disconnect users and shut down the server

c. prevent any new users from logging on

d. notify all users that they must finish their work immediately and log off

13. Which of the following is not a characteristic of a disaster recovery plan (DRP)?

a. It is updated regularly.

b. It is a private document only used by top-level administrators for planning. – PG491-493

c. It is written.

d. It is detailed.

14. Any time the contents of a file are changed, the archive bit is changed to \_\_\_\_, meaning that this modified file now needs to be backed up.

a. 0

b. 1 – PG501

c. 2

d. 3

15. An incremental backup \_\_\_\_\_\_.

a. copies selected files

b. copies all files

c. copies all files since the last full backup

d. copies all files changed since the last full or incremental backup – PG502

16. Each of the following is a basic question to be asked regarding creating a data backup except: \_\_\_\_\_\_\_.

a. How long will it take to finish the backup? – PG501

b. Where should the backup be stored?

c. What information should be backed up?

d. What media should be used?

17. The chain of \_\_\_\_\_\_ documents that the evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt the evidence.

a. forensics

b. evidence

c. control

d. custody – PG510

18. \_\_\_\_\_\_\_is the maximum length of time that an organization can tolerate between data backups.

a. Recovery service point (RSP)

b. Recovery point objective (RPO) – PG503

c. Optimal recovery time frame (ORT)

d. Recovery time objective (RTO)

19. A data backup solution that uses a magnetic disk as a temporary storage area is \_\_\_\_\_\_\_.

a. disk to disk to tape (D2D2T) – PG503

b. disk to disk (D2D)

c. tape to disk (T2D)

d. continuous data protection (CDP)

20. When an unauthorized event occurs, the first duty of the computer forensics response should be to \_\_\_\_\_\_.

a. log off the server

b. secure the crime scene – PG510

c. back up the hard drive

d. reboot the system

1. A statement regarding due diligence would be found in which security policy?

a. Disposal and destruction policy

b. Acceptable use policy

c. Privacy policy

d. Security-related human resource policy – PG547

2. Which risk category addresses events that impact the daily business of the organization?

a. Strategic

b. Operational – PG536

c. Tactical

d. Daily

3. \_\_\_\_\_\_\_\_\_ management covers the procedures of managing object authorizations.

a. Privilege – PG536

b. Threat

c. Task

d. Asset

4. Which of the following is not a characteristic of a policy?

a. Policies communicate a unanimous agreement of judgment. – PG541

b. Policies may be helpful in the event that it is necessary to prosecute violators.

c. Policies identify what tools and procedures are needed.

d. Policies define appropriate user behavior.

5. Which of the following is not an approach to trust?

a. Trust all people all the time. – PG40

b. Trust everyone all of the time.

c. Trust authorized individuals only.

d. Trust some people some of the time.

6. \_\_\_\_\_\_\_\_\_ is defined as the obligations that are imposed on owners and operators of assets to exercise reasonable care of the assets and take necessary precautions to protect them.

a. Due care – PG543

b. Due obligations

c. Due process

d. Due diligence

7. What is a collection of suggestions that should be implemented?

a. Policy

b. Guideline – PG540

c. Standard

d. Code

8. Each of the following is a guideline for developing a security policy except \_\_\_\_\_\_\_.

a. notify users in advance that a new security policy is being developed and explain why the policy is needed

b. require all users to approve the policy before it is implemented – PG544

c. provide a sample of people affected by the policy with an opportunity to review and comment

d. prior to deployment, give all users at least two weeks to review and comment

9. Each of the following is what a security policy must do except \_\_\_\_\_\_.

a. balance protection with productivity

b. be able to implement and enforce it

c. state reasons the policy is necessary – PG542

d. be concise and easy to understand

10. Which of the following should not serve on a security policy development team?

a. Senior level administrator

b. Member of the legal staff

c. Member of management who can enforce the policy

d. Representative from a hardware vendor – PG543

11. Which policy defines the actions users may perform while accessing systems and net- working equipment?

a. End-user policy

b. Internet use policy

c. User permission policy

d. Acceptable use policy – PG544

12. \_\_\_\_\_\_ may be defined as the study of what people understand to be good and right behavior and how people make those judgments.

a. Morals

b. Values

c. Ethics – PG549

d. Principles

13. A classification of information policy is designed to produce a standardized framework for classifying \_\_\_\_\_\_.

a. information assets – PG549

b. types of policies

c. user password violations

d. free hard drive

14. Which of the following would be found in a password management and complexity policy?

a. Do not use alphabetic characters.

b. Do not use a password that is a word found in a dictionary.

c. Do not use the name of a pet.

d. Do not use personally identifiable information. – PG548

15. Which of the following is true regarding a privacy policy?

a. It covers the same material as that found in an AUP.

b. It must be certified before it can be used.

c. It is required on all Internet Web sites.

d. It is also called a personally identifiable information policy. – PG546

16. Which is not one of the challenges in a classification of information policy?

a. The number of supervisors needed to oversee the work. – PG549

b. There is a tendency to create multiple levels of classification.

c. There are attempts to use information classification categories developed by another organization and “force” them to fit.

d. The desire to classify all items as high security.

17. For adult learners, a(n) \_\_\_\_\_\_\_ approach (the art of helping an adult learn) is often preferred.

a. andragogical – PG555

b. institutional

c. proactive

d. pedagogical

18. Requiring employees to clear their workspace of all papers at the end of each business day is called \_\_\_\_\_\_\_.

a. empty workspace policy

b. clean desk policy – PG551

c. disposal and removal policy

d. sunshine policy

19. What is the security risk of a P2P network?

a. A virus can be transmitted. – PG552

b. It consumes bandwidth.

c. It allows law enforcement agencies to monitor the user’s actions.

d. It is issued to spread spam.

20. Which of the following is not a general security recommendation when using social networking sites?

a. Consider carefully who is accepted as a friend.

b. Show “limited friends” a reduced version of your profile.

c. Only access a social networking site on personal time. – PG553

d. Disable options and then reopen them only as necessary.