Name: _____ **Class:** _____ **Date:** _____ **ID: A**

Pop Quiz #1

Multiple Choice
Identify the choice that best completes the statement or answers the question.

1. Databases fit into which of the following categories?
   a. Data/Information
   b. Software
   c. Hardware
   d. All of the Above

2. Which of the following is a security risk regarding the use of public P2P as a method of collaboration?
   a. Data integrity is susceptible to being compromised.
   b. Monitoring data changes induces a higher cost.
   c. Users are not responsible for data usage tracking.
   d. Limiting the amount of necessary space for data storage.

3. A network administrator has purchased two devices that will act as failovers for each other. Which of the following concepts does this BEST illustrate?
   a. Authenticity
   b. Confidentiality
   c. Integrity
   d. Availability

4. A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?
   a. Confidentiality
   b. Availability
   c. Succession Planning
   d. Integrity

5. Which of the following concepts describes the use of a one way transformation in order to validate the integrity of a program?
   a. Hashing
   b. Key Escrow
   c. Non-Repudiation
   d. Steganography

6. Sara, a security administrator, manually hashes all network device configuration files daily and compares them to the previous days' hashes. Which of the following security concepts is Sara using?
   a. Confidentiality
   b. Compliance
   c. Integrity
   d. Availability

7. A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:
   a. Integrity of downloaded software.
   b. Availability of the FTP site.
   c. Confidentiality of downloaded software.
   d. Integrity of the server logs.

8. It is important to staff who use email messaging to provide PII to others on a regular basis to have confidence that their messages are not intercepted or altered during transmission. They are concerned about which of the following types of security control?
   a. Integrity
   b. Safety
   c. Availability
   d. Confidentiality

Multiple Response
Identify one or more choices that best complete the statement or answer the question.

9. Which of the following concepts are included on the three sides of the "security triangle"? (Select THREE).
   a. Confidentiality
   b. Integrity
   c. Availaibility
   d. Authentication
   e. Authorization
   f. Continuity

10. Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?
    a. Cognitive password
    b. Password sniffing
    c. Brute force
    d. Social engineering

Pop Quiz #1
Answer Section

MULTIPLE CHOICE

1. ANS: A
   Databases are made of data that interact with hardware and software.

   PTS: 1
2. ANS: A
   Peer-to-peer (P2P) networking is commonly used to share files such as movies and music, but you must not allow users to bring in devices and create their own little networks. All networking must be done through administrators and not on a P2P basis. Data integrity can easily be compromised when using public P2P networking.

   PTS: 1
3. ANS: D
   Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored. In the case of a network, this means processing switches to another network path in the event of a network failure in the primary path. This means availability.

   PTS: 1
4. ANS: B
   Simply making sure that the data and systems are available for authorized users is what availability is all about. Data backups, redundant systems, and disaster recovery plans all support availability. And creating a hot site is about providing availability.

   PTS: 1
5. ANS: A
   Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and its main characteristics are:
   It must be one-way – it is not reversible.
   Variable-length input produces fixed-length output – whether you have two characters or 2 million, the hash size is the same.
   The algorithm must have few or no collisions – in hashing two different inputs does not give the same output.

   PTS: 1
6. ANS: C
   Integrity means the message can't be altered without detection.

   PTS: 1

7. ANS: A
   Digital Signatures is used to validate the integrity of the message and the sender. In this case the software firm that posted the patches and updates digitally signed the checksums of all patches and updates.

   PTS: 1
8. ANS: A
   Integrity means that the messages/ data is not altered. PII is personally identifiable information that can be used to uniquely identify an individual. PII can be used to ensure the integrity of data/messages.

   PTS: 1

MULTIPLE RESPONSE

9. ANS: A, B, C
   The CIA is Confidentiality, Integrity, and Availability. Authentication & Authorization are the processes of obtaining access. Continuity is based on continuity of operations.

   PTS: 1
10. ANS: C
    One way to recover a user's forgotten password on a password protected file is to guess it. A brute force attack is an automated attempt to open the file by using many different passwords.
    A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security. A brute force attack may also be referred to as brute force cracking. For example, a form of brute force attack known as a dictionary attack might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers. An attack of this nature can be time- and resource-consuming. Hence the name "brute force attack;" success is usually based on computing power and the number of combinations tried rather than an ingenious algorithm.

    PTS: 1