MIS5206 – Unit 5a Name:_____

1. A network administrator must grant the appropriate network permissions to a new employee. Which of the following is the best strategy?
    a. Give the new employee user account the necessary rights and permissions.
    b. Add the new employee user account to a group. Ensure the group has the necessary rights and permissions.
    c. Give the new employee administrative rights to the network.
    d. Ask the new employee what network rights they would like.

2. In securing your network, you enforce complex user passwords. Users express concern about forgetting their passwords. What should you configure to allay those concerns?
    a. Password expiration
    b. Periodic password change
    c. Password hints
    d. Maximum password length

3. To quickly give a contractor network access, a network administrator adds the contractor account the Windows Administrative group. Which security principle does this violate?
    a. Separation of duties
    b. Least privilege
    c. Job rotation
    d. Account lockout

4. A secure computing environment labels data with various security classifications. Authenticated users must have clearance to read this classified data. What type of access control model is this?
    a. Mandatory access control
    b. Discretionary access control
    c. Role-based access control
    d. Time-of-day access control

5. To ease giving access to network resources for employees, you decide there must be an easier way than granting users individual access to files, printers, computers, and applications. What security model should you consider using?
    a. Mandatory access control
    b. Discretionary access control
    c. Role-based access control
    d. Time-of-day access control

6. Linda creates a folder called Budget Projections in her home account and shares it with colleagues in her department. Which of the following best describes this type of access control system?
    a. Mandatory access control
    b. Discretionary access control
    c. Role-based access control
    d. Time-of-day access control

7. You require that users not be logged on to the network after 6 PM while you analyze network traffic during nonbusiness hours. What should you do?
    a. Unplug their stations from the network
    b. Tell users to press CTRL-ALT-DEL to lock their stations
    c. Configure time-of-day restrictions to ensure nobody can be logged in after 6 PM
    d. Disable user accounts at 6 PM

8. One of your users, Matthias, is taking a 3-month leave of absence because of a medical condition, after which he will return to work. What should you do with Matthias' user account?
    a. Delete the account and re-create it when he returns
    b. Disable the account and enable it when he returns
    c. Export his account properties to a text file for later import and then delete it
    d. Ensure you have a backup of his account details and delete his account

9. During an IT security meeting, the topic of account lockout surfaces. When you suggest all users accounts be locked for 30 minutes after three incorrect logon attempts, your colleague Phil states this is a serious problem when applied to administrative accounts. What types of issues might Phil be referring to?
    a. Dictionary attacks could break into administrative accounts
    b. Administrative accounts are much sought after by attackers
    c. Administrative accounts are placed into administrative groups
    d. DoS attacks could render administrative accounts unusable

10. What type of attack is mitigated by strong, complex passwords?
    a. DoS
    b. Dictionary
    c. Brute force
    d. DNS poisoning

11. A government contract requires your computers to adhere to mandatory access control methods and multilevel security. What should you do to remain compliant with this contract?
    a. Patch your current operating system
    b. Purchase new network hardware
    c. Use a trusted OS
    d. Purchase network encryption devices

12. Which term is best defined as an object's list of users, groups, processes, and their permissions?
    a. ACE
    b. ACL
    c. Active Directory
    d. Access log