1. Which of the following is not considering the adequate measure for physical security?
a) Lock the drawers
b) Keep strong passwords for corporate laptops and mobile phones
*c) Keep confidential organization's document file open in the desk
d) Hide your hand against camera while inserting the PIN code

2. Which of the following is not a physical security measure to protect against physical hacking?
a) Add front desk & restrict unknown access to the back room
b) Create a phishing policy
c) Analyze how employees maintain their physical data and data storage peripheral devices
*d) Updating the patches in the software you're working at your office laptop.

3. Use of _____ can bring external files and worms and virus along with it to the internal systems.
a) smart-watch
*b) pen drive
c) laptop
d) iPod

4. Which security control below doesn't belong to the group of the other three?

*A. Host-based intrusion-detection system
B. Photoelectric system
C. Acoustical-seismic detection system
D. Passive infrared system

5. Which of the following characteristics is not true of an ideal data-processing room?

A. The room has a humidity level of 50%.
*B. The room has carpeting.
C. The temperature of the room is around 72 degrees Fahrenheit.
D. The room has independent HVAC and ventilation systems.

6. A security system that uses changes in heat waves in a particular area to identify possible intruders is called a _____.

A. Proximity detection system
*B. Passive infrared system
C. Acoustical-seismic detection system
D. Photometric system

7. Doors configured in a fail-safe mode assume what position in the event of a power failure?

A. Open and locked
B. Closed and locked
*C. Closed and unlocked
D. Open

8. Piggybacking can be prevented best by which physical control?

A. Turnstile
*B. Mantrap
C. Badge reader
D. Fail-safe door

9. Perimeter protection, area/space protection, and object/spot protection are categories of:
a. Crime pattern analysis
b. Risk management
*c. Sensing device
d. None of the above