**Chapter 16 – Physical and Infrastructure Security**

**TRUE/FALSE QUESTIONS:**

T F 1. To implement a physical security program an organization must

conduct a risk assessment to determine the amount of resources to devote to physical security and the allocation of those resources against the various threats.

T F 2. Physical security must also prevent any type of physical access or

intrusion that can compromise logical security.

T F 3. For information systems, the role of logical security is to protect the

physical assets that support the storage and processing of information.

T F 4. Physical security must prevent misuse of the physical infrastructure

that leads to the misuse or damage of the protected information.

T F 5. Misuse of the physical infrastructure includes vandalism, theft of

equipment, theft by copying, theft of services, and unauthorized entry.

T F 6. The optimal temperature for computer systems is between 10 and 32

degrees Fahrenheit.

T F 7. High humidity does not pose a threat to electrical and electronic

equipment as long as the computer’s temperature stays within the optimal range.

T F 8. If a computer’s temperature gets too cold the system can undergo

thermal shock when it is turned on.

T F 9. A person that becomes statically charged can damage electronic

equipment by an electric discharge.

T F 10. The direct flame is the only threat from fire.

T F 11. Low-intensity devices such as cellular telephones do not interfere with

electronic equipment.

T F 12. Human-caused threats are less predictable than other types of physical

threats.

T F 13. Unauthorized physical access can lead to other threats.

T F 14. Physical access control should address not just computers and other IS

equipment but also locations of wiring used to connect systems, equipment and distribution systems, telephone and communications lines, backup media, and documents.

T F 15. The CHUID is a PIV card data object.

**MULTIPLE CHOICE QUESTIONS:**

1. \_\_\_\_\_\_\_\_ security protects computer-based data from software-based and communication-based threats.

A. Infrastructure B. Premises

C. Physical D. Logical

2. \_\_\_\_\_\_\_\_ security provides perimeter security, access control, smoke and fire detection, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards.

A. Premises B. Infrastructure

C. Logical D. Physical

3. \_\_\_\_\_\_\_\_ includes data processing and storage equipment, transmission and networking facilities, and offline storage media.

A. Supporting facilities B. Physical facilities

C. Information system hardware D. Infrastructure facilities

4. \_\_\_\_\_\_\_ facilities include electrical power, communication services, and environmental controls such as heat and humidity.

A. Supporting B. Information

C. Physical D. All of the above

5. Relative humidity should be maintained between \_\_\_\_\_\_\_\_ to avoid the threats from both low and high humidity.

A. 20% and 80% B. 40% and 60%

C. 50% and 50% D. 30% and 70%

6. A prevalent concern that is often overlooked is \_\_\_\_\_\_\_\_.

A. overvoltage B. undervoltage

C. dust D. noise

7. \_\_\_\_\_\_\_\_ threats are specifically designed to overcome prevention measures and seek the most vulnerable point of attack.

A. Human-caused B. Technical

C. EMI D. Environmental

8. Eavesdropping and wiretapping fall into the \_\_\_\_\_\_\_\_ category.

A. theft B. vandalism

C. misuse D. unauthorized physical access

9. \_\_\_\_\_\_\_ includes destruction of equipment and data.

A. Misuse B. Vandalism

C. Theft D. Unauthorized physical access

10. \_\_\_\_\_\_\_ should be located on the floor of computer rooms as well as under raised floors, and should cut off power automatically in the event of a flood.

A. Smoke detectors B. UPS

C. Water sensors D. Equipment power off switches

11. The \_\_\_\_\_\_ is an optional key that may be present on any PIV card, does not require PIN entry, and whose purpose is to authenticate the card and therefore its possessor.

A. VIS B. BIO

C. CHUID D. CAK

12. The role of physical security is affected by the operating location of the information system, which can be characterized as \_\_\_\_\_\_ .

A. static B. portable

C. mobile D. all of the above

13. An area of a facility that has no security interest is classified as \_\_\_\_\_\_\_\_\_.

A. unrestricted B. controlled

C. limited D. exclusion

14. A restricted area within close proximity of a security interest has a classification of \_\_\_\_\_\_.

A. exclusion B. controlled

C. limited D. unrestricted

15. The security classification for a restricted area containing a security interest is \_\_\_\_\_.

A. controlled B. exclusion

C. unrestricted D. limited

**SHORT ANSWER QUESTIONS:**

1. \_\_\_\_Physical\_\_\_\_\_ security, also called infrastructure security, protects the information systems that contain data and the people who use, operate, and maintain the systems.
2. Physical security threats are organized into three categories: environmental threats, human-caused threats, and \_\_\_\_\_technical\_\_\_\_ threats.
3. Tornados, tropical cyclones, earthquakes, blizzards, lightning, and floods are all types of \_\_\_\_\_natural\_\_\_ disasters.
4. \_\_\_environmental\_\_\_\_\_\_ threats encompass conditions in the environment that can damage or interrupt the service of information systems and the data they contain.
5. \_\_\_\_technical\_\_\_ threats encompass threats related to electrical power and electromagnetic emission.
6. Power utility problems can be grouped into three categories: under voltage, overvoltage, and \_\_\_noise\_\_\_\_\_.
7. An \_\_under voltage\_\_\_\_\_ condition occurs when the IS equipment receives less voltage than is required for normal operation.
8. \_\_\_human-caused\_\_\_\_\_ physical threats are more difficult to deal with than environmental and technical threats.
9. Human-caused threats can be grouped into the following categories: unauthorized physical access, theft, \_\_\_\_vandalism\_\_\_\_\_ and misuse.
10. Noise along a power supply line, motors, fans, heavy equipment, microwave relay antennas, and other computers are all sources of \_\_\_electromagnetic interference (EMI)\_\_\_\_\_\_.
11. To deal with the threat of smoke, the responsible manager should install \_\_\_smoke detectors\_\_\_\_ in every room that contains computer equipment as well as under raised floors and over suspended ceilings.
12. A(n) \_\_\_uninterruptible power supply (UPS)\_\_\_\_\_ is a battery backup unit that can maintain power to processors, monitors, and other equipment and can also function as a surge protector, power noise filter, and an automatic shutdown device.
13. The most essential element of recovery from physical security breaches is \_redundancy\_\_\_.
14. \_\_\_biometric (BIO)\_\_\_ authentication is implemented by using a fingerprint or iris data object sent from the PIV card to the PACS.
15. The \_\_attended biometric (BIO-A)\_\_\_\_\_ authentication has an attendant supervise the use of the PIV card and the submission of the PIN and the sample biometric by the cardholder.