MICAD LIMITED
Advanced Industrial Security Supervisor Training

Lesson 4.4: Activity: Designing an Access Control System

For this activity, you will design an access control system for a specific area within a hypothetical industrial facility. Choose ONE of the following areas, or select another area relevant to industrial security:

- Manufacturing Plant Floor (specify a particular section, e.g., assembly line, packaging area, server room)
- Data Center (specify a particular area, e.g., server room, network closet, restricted area)
- Power Substation (specify a particular area, e.g., control room, transformer yard, battery room)
- Chemical Plant (specify a particular area, e.g., control room, processing area, storage facility)
- Hospital (specify a particular area, e.g., operating room, server room, pharmacy)

Your design should include the following elements:

1. **Area Description:** Briefly describe the chosen area, including its size, purpose, and the types of personnel who require access.

2. Risk Assessment: Conduct a brief risk assessment, considering potential threats and vulnerabilities specific to this area. What are you trying to protect? What are the potential risks associated with unauthorized access?

3. Technology Selection: Choose appropriate access control technologies for this area. Consider using a combination of technologies if appropriate. Justify your choices based on the risk assessment. For example:

- **Physical Access Control:** Keypads, card readers (magnetic stripe, smart card, proximity), biometric scanners (fingerprint, iris, facial recognition), security guards, turnstiles, gates, locks.
- **Logical Access Control:** Passwords, multi-factor authentication (MFA), role-based access control (RBAC), access control lists (ACLs), network security devices (firewalls).

4. Credential Management: Outline procedures for managing access credentials (issuance, revocation, replacement, lost/stolen credentials). What are the processes for requesting access, assigning credentials, and revoking access?

5. Access Levels: Define different access levels based on the roles and responsibilities of personnel. Consider using a hierarchical approach with different levels of authorization. For example, administrators might have full access, while regular employees have limited access to specific areas or systems.

6. Integration with Other Systems: Describe how the access control system integrates with other security measures in place (e.g., CCTV, alarm systems, intrusion detection systems). How will the access control system trigger alerts or recordings in other systems?

7. Monitoring and Auditing: Describe procedures for monitoring access logs and conducting regular audits to ensure compliance. How will you track who accesses the chosen area? How often will audits be conducted?

8. Incident Response: Outline procedures for responding to unauthorized access attempts or breaches. What are the steps that will be taken if there is an unauthorized access?

9. Training: Specify training requirements for all personnel covered by this access control system.

10. Legal and Ethical Considerations: Address any relevant legal or ethical considerations (e.g., data privacy when using biometrics).

Submission:

Submit your access control system design in the Discussion panel. Your design should be clear, concise, well-organized, and reflect your understanding of best practices for access control. Include diagrams,

if possible, to illustrate your proposed layout. Engage with your classmates by offering feedback on their designs.

This detailed framework will assist students in creating a comprehensive and well-structured access control system design. The requirement to justify technology selections based on a specific risk assessment will further reinforce the application of learned concepts. The discussion panel encourages collaborative learning and the exchange of ideas. Consider limiting the number of technologies employed to avoid overwhelming designs.