



MICAD LIMITED
Advanced Industrial Security Supervisor Training

Lesson 3.2: Activity - Developing a Draft Access Control Security Policy

Here's a framework to guide students in completing the activity:

"Develop a draft access control policy for a specific area within a hypothetical industrial facility." This framework can be provided to students to help them structure their submission to the discussion panel.

Activity: Developing a Draft Access Control Policy

For this activity, you will develop a draft access control policy 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 policy should address BOTH physical and logical access control and include the following elements:

1. **Policy Title and Purpose:** Clearly state the policy's title and its overall purpose. What is this policy designed to protect?

2. **Scope:** Define the scope of the policy. What specific areas, systems, or data does it cover? Be specific. (e.g., "This policy applies to all personnel accessing the Server Room on Floor 3 of the manufacturing facility.")

3. **Definitions:** Define key terms (e.g., "authorized personnel," "restricted area," "logical access").

4. **Physical Access Control:**

- Describe the physical access control measures in place (e.g., security doors, locks, keycard readers, security guards, surveillance cameras).
- Outline procedures for obtaining and managing physical access credentials (e.g., keycard issuance, access requests, lost or stolen credentials).
- Specify access levels and restrictions for different areas. (e.g., "Only authorized personnel with appropriate clearance may enter the server room.")

5. **Logical Access Control:**

- Describe the logical access control measures in place (e.g., strong passwords, multi-factor authentication, role-based access control, firewalls).
- Outline procedures for managing user accounts and access rights (e.g., account creation, modification, deletion).
- Specify access levels and restrictions for different systems and data. (e.g., "Only administrators have full access to the database server.")

6. **Responsibilities:** Clearly assign roles and responsibilities for implementing and enforcing the policy. (e.g., "The Security Supervisor is responsible for overseeing the physical access control system. The IT Manager is responsible for managing logical access.")

7. Monitoring and Auditing: Describe procedures for monitoring access logs and conducting regular audits to ensure compliance.

8. Incident Response: Outline procedures for responding to unauthorized access attempts or breaches.

9. Training: Specify training requirements for all personnel covered by the policy.

10. Policy Review and Updates: Establish a schedule for regular review and updates of the policy to address changes in the organization or the threat landscape.

Addressing Potential Challenges:

Your policy should also address potential challenges in implementing and managing the access control system. For example, how will you handle:

- Lost or stolen credentials?
- User resistance to new security measures?
- Integration of various systems?
- Escalating access requests?

Submission:

Post your draft access control policy in the discussion panel. Your submission should be well-organized, clearly written, and demonstrate your understanding of best practices for access control. Engage with your classmates' submissions by providing constructive feedback.

This framework provides a structured approach to creating a comprehensive access control policy. The inclusion of specific details for your chosen facility and consideration of potential challenges will demonstrate a high level of understanding of access control principles and practices. Leverage your previous learning on risk assessment and policy development. The discussion forum is designed to allow for peer-to-peer learning and feedback.