



MICAD LIMITED
Advanced Industrial Security Supervisor Training

Lesson 3.1: Activity - Developing a Draft Security Policy

Here's a framework to guide you in completing the activity: "Develop a draft security policy addressing a specific area of concern for a hypothetical industrial setting." Submit to the discussion panel.

Activity: Developing a Draft Security Policy

For this activity, you will develop a draft security policy addressing a specific area of concern for a hypothetical industrial setting. Choose ONE of the following areas of concern, or select another area relevant to industrial security:

- Access Control
- Data Security
- Incident Response
- Physical Security
- Cybersecurity (Network Security)
- Personnel Security

- Supply Chain Security

Your policy should include the following elements:

1. **Policy Title and Purpose:** Clearly state the policy's title and its overall purpose. Explain what this policy aims to achieve in terms of security for the chosen area.
2. **Scope:** Define the scope of the policy. Which parts of the organization, systems, or personnel does this policy apply to? Be specific.
3. **Definitions:** Define any key terms or concepts used in the policy. This will help to ensure clarity and consistency.
4. **Policy Statements:** This section outlines the specific rules and regulations related to your chosen area of concern. Be clear, concise, and avoid ambiguity. Use actionable language.
5. **Procedures:** For each policy statement, describe the procedures to be followed. Explain the steps individuals should take to comply with the policy.

6. **Responsibilities:** Specify the roles and responsibilities of different individuals or departments in implementing and enforcing the policy.
7. **Enforcement:** Describe the mechanisms for monitoring compliance and the consequences of non-compliance. Ensure fairness and consistency.
8. **Review and Updates:** Establish a schedule for reviewing and updating the policy (e.g., annually, or when significant changes occur).
9. **Legal and Ethical Considerations:** Address any relevant legal or ethical considerations related to your chosen area. For example, data security policies need to address privacy regulations (e.g., GDPR, CCPA, HIPAA).
10. **Integration with Other Policies:** Briefly explain how this policy integrates with other relevant security policies within the organization.

Hypothetical Setting:

You can create a hypothetical industrial setting (e.g., a manufacturing plant, a power substation, a data center, a hospital) or use the "SunPeak" solar power substation used in previous lessons.

Submission:

Post your draft security policy in the Discussion panel. Your submission should be well-organized, clearly written, and reflect your understanding of the lesson material. Engage with your classmates' submissions by commenting on their policies and offering constructive feedback. Be sure to address the ten points listed above.

This detailed framework provides a robust structure for creating a comprehensive security policy. By addressing all ten points, you demonstrate a thorough understanding of policy development and implementation. Draw upon your previous learning around threat modeling, risk assessment, and legal/ethical considerations in developing this draft policy. The discussion panel allows for collaborative learning and feedback.