CIP-006-6 R2

Security Objective

The organization monitors physical access to the protected systems in addition to the physical access monitoring of the facility of organization-defined physical spaces containing one or more components of the protected systems.

Develops, documents, and disseminates to organization: 1) A physical and protection policy that addresses visitor escort and authorization

NIST Special Publication 800-53 (Rev. 4) PE-1, 2, 3, 6(1, 2)

WECC Intent

The potential failure points and guidance questions provide general direction to registered entities for assessment of risk while designing internal controls specific to NERC Reliability Standards and Requirements. The Registered Entity may use this document as a starting point in determining entity risk and it is not WECC's intent to establish a standard or baseline for entity risk assessment or controls design.

Note: *Guidance Questions serve to aid an entity in understanding and/or documenting its controls. Any responses, including lack of affirmative feedback, will have no consequences to an entity's demonstration of compliance at audit.*

**Please feel free to provide feedback to ICE@WECC.org with suggestions on Potential Failure Points & Guidance Questions.*

Potential Failure Points & Guidance Questions

Potential Failure Point: (R2) Failure to develop a policy that requires continuous escort

1. How has your entity communicated the requirement to provide continuous escort where applicable?
2. How has your entity made employees aware of the policy that requires continuous escort?
3. Does your entity have any controls to detect a failure of continuous escort?

Potential Failure Point: (R2) Failure to develop a process to identify a visitor who is not authorized

1. How does your entity differentiate between individuals with authorized unescorted physical access and visitors who require escort?
2. How does your entity ensure that individuals escorting visitors are aware of their responsibilities?
3. Describe how your entity ensures escorts provide continuous monitoring of the visitor.
    a. If an escort fails to perform their duties, how is this detected?
4. Describe how your entity determines which individuals are qualified to provide visitor escort.
    a. For instance, does your entity maintain any qualifying criteria for who can be an escort?
        i. If so, how does your entity ensure that your criteria or review process has been adhered to?
        ii. If so, how often is the criteria reviewed for accuracy?
5. How does your entity process address CIP visitors who arrive unplanned or on short notice?
    a. How does your entity validate a business need for access during an unplanned or short notice visit?

Potential Failure Point: (R2) Failure to develop criterion for qualifying a CIP Exceptional Circumstance.

1. How does your entity ensure that a CIP Exceptional Circumstance is officially determined prior to allowing access?
2. How does your entity document CIP Exceptional Circumstances?

Potential Failure Point: (R2) Failure to develop a policy that requires manual or automated logging of visitor entry into and exit from the Physical Security Perimeter

1. How has your entity communicated the requirement to provide manual or automated logging?
2. How does your entity ensure all personnel know the processes to perform manual or automated logging?
3. How does your entity consolidate manual and automated logs?

Potential Failure Point: (R2) Failure to develop a procedure on how to document minimally required data for visitors

1. How does your entity record date and time of the initial, entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor?
    a. How does your entity review logs for quality (content, readability and completeness)?
    b. How does your entity ensure that logs are completed for remote locations?

   c. Describe any training or job aides (such as a checklist) that ensure that personnel are aware of how visits should be logged.
   d. How does your entity ensure that personnel complete the logs of visitor entry and exit
      i. For example, is security notified of the visit and that logs have been completed?
2. How does your entity confirm the visitor's identity?
3. How does your entity address logs with inaccurate or missing information?
4. Does your entity provide training on manual logging requirements?

Potential Failure Point (R2) Failure to develop a process to collect and retain visitor logs

1. How does your entity ensure logs are collected?
2. How does your entity ensure logs are retained for at least ninety calendar days?
3. If an automated system is used for logging, what process does your entity have to ensure that the system is properly configured to meet the requirements of 2.2 and 2.3?
4. If a manual process is used for logging, what process does your entity have to ensure that the logs are protected from loss or unauthorized change?