Electric Reliability and Security for the West

Internal Controls
Failure Points and Guidance Questions
CIP-004-6 R5

Security Objective

- Develop processes that establish and enforce revoking access due to changes to the business need for access.
- Ensure electronic access to BES Cyber Systems is promptly revoked per standards. Process to address all situations in which there is an involuntary change of assignment or employment.

NIST Special Publication 800-53 (Rev. 4) AC-3(8)

WECC Intent

The potential failure points and guidance questions give 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. It is not WECC's intent to establish a standard or baseline for entity risk assessment or controls design.

Note: *Guidance questions help an entity understand and document its controls. Any responses, including lack of affirmative feedback, will have no consequences on an entity's demonstration of compliance at audit.*

**Please send feedback to ICE@WECC.org with suggestions on potential failure points and guidance questions.*

Potential Failure Points & Guidance Questions

Potential Failure Point: Failure to develop a process to accurately inventory access and accounts.

1. How do you ensure the inventory of individuals, their access, and accounts that subject to R5 revocation is complete and up to date?
    a. Do you have a defined process to identify all access that an individual has?

Potential Failure Point: Failure to develop a process to track and communicate a change in employment status (termination, reassignment, or transfer action) to all personnel involved in access revocation processes.

1. How do you ensure that everyone who must be notified of a termination, reassignment, or transfer is notified?
    a. Do you have a process to verify that they have received the information?
    b. If the responsible person is not available to take action, how do you ensure they have qualified backup?

Potential Failure Point: Failure to define a process to authorize access.

1. Has you defined what constitutes a record of authorization?
    a. How do you ensure that authorization records are documented consistently?
2. Have you defined workflows that show the authorization process?
3. How are personnel responsible for authorizing access made aware of their responsibilities?

Potential Failure Point: Failure to develop a process for designating and identifying storage locations for BES Cyber System Information.

1. How have you defined physical storage locations?
2. How have you defined electronic storage locations?
3. What is your process for identifying information that qualifies as BES Cyber System Information?
4. What is your process to document designated storage locations for BES Cyber System Information?
    a. What is your process to ensure the list of storage locations is kept up to date?
5. How do you ensure that all contractors or service vendors are aware of defined BES Cyber System Information?
    a. What controls are in place to ensure PRA and training have been conducted before access is given?

Potential Failure Point: Failure to develop a procedure on how to perform quarterly and 15-calendar month verifications.

1. How have you established a method to determine authorized access?
    a. Does your procedure consider a separation of duties for verifications?
2. How have you established a method to determine actual access?
    a. How do you ensure all actual access is considered during the review process?
    b. How do you ensure the correct privileges are being reviewed?
    c. How do you document the results of the reviews?

Potential Failure Point: Failure to clearly define or communicate start and end dates used to establish timeframes in the verification process.

1. How does each line of business establish these start and end dates for verifications?