

**Reliability Standard Audit Worksheet for British Columbia**

# CIP-004-5.1 – Cyber Security – Personnel & Training

# Reliability Standard Effective Date for BC: October 1, 2018

***The Compliance Monitor Administrator must complete this section***

**Registered Entity:** [Name & ACRO]

**WCR Number:** WCRXXXXX

**Compliance Assessment Date:** [Audit start date – audit end date]

**Compliance Monitoring Method:** [Audit Type]

**Applicable Function(s):** BA, DP, GO, GOP, TO, TOP

**Names of Auditors:**

Findings Table:

|  |  |  |  |
| --- | --- | --- | --- |
| Req. | Finding | Summary and Documentation | Functions Monitored |
| [R1](#R1_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |
| [R2](#R2_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |
| [R3](#R3_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |
| [R4](#R4_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |
| [R5](#R5_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |

|  |  |
| --- | --- |
| Req. | Areas of Concern |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| Req. | Recommendations |
|  |  |
|  |  |
|  |  |

# **Subject Matter Experts**

Identify subject matter expert(s) responsible for this Reliability Standard. Insert additional lines if necessary.

**Registered Entity Response (Required):**

|  |  |  |  |
| --- | --- | --- | --- |
| **SME Name** | **Title** | **Organization** | **Requirement(s)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**R1 Supporting Evidence and Documentation**

**R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

**M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| **CIP-004-5.1 Table R1 – Security Awareness Program** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | High Impact BES Cyber Systems  Medium Impact BES Cyber Systems | Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. | An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as:   * direct communications (for example, e-mails, memos, computer-based training); or * indirect communications (for example, posters, intranet, or brochures); or * management support and reinforcement (for example, presentations or meetings). |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 1.1

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes which include security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. |
|  | Verify the Responsible Entity has reinforced security awareness at least once each calendar quarter. |
|  | Verify the security awareness reinforcement included:   * reinforcement of cyber security practices, or * reinforcement of physical security practices associated with cyber security. |
|  | Verify that security awareness was reinforced for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. |
| **Note to Auditor:**  The Responsible Entity is not required to document that each quarter’s reinforcement was received by each of its authorized personnel. Rather, the Responsible Entity is required to demonstrate that the security awareness reinforcement was communicated to its authorized personnel as a whole, not necessarily individually. | |

[**Compliance Summary:**](#R1)

|  |
| --- |
| Finding Summary:  Primary Documents Supporting Findings: |

**Auditor Notes:**

|  |
| --- |
|  |

R2 Supporting Evidence and Documentation

**R2.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5.1 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

**M2.** Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5.1 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

| **CIP-004-5.1 Table R2 – Cyber Security Training Program** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Training content on:  2.1.1. Cyber security policies;  2.1.2. Physical access controls;  2.1.3. Electronic access controls;  2.1.4. The visitor control program;  2.1.5. Handling of BES Cyber System  Information and its storage;  2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan;  2.1.7. Recovery plans for BES Cyber  Systems;  2.1.8. Response to Cyber Security  Incidents; and  2.1.9. Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets. | Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 2.1

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify that the training program(s) collectively include content on the following:   1. Cyber security policies; 2. Physical access controls; 3. Electronic access controls; 4. The visitor control program; 5. Handling of BES Cyber System Information and its storage; 6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan; 7. Recovery plans for BES Cyber Systems; 8. Response to Cyber Security Incidents; and 9. Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media. |
|  | Verify the Responsible Entity’s training program’s content is appropriate to individual roles, functions, or responsibilities. |
| **Notes to Auditor:**   1. The training program(s) must collectively include all nine training elements. 2. It is not necessary that all nine training elements be included for the training of each role, function, or responsibility. 3. Each role, function, or responsibility must receive training on all appropriate training elements. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R2 – Cyber Security Training Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.2 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances. | Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 2.2

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify all personnel completed the training specified in Part 2.1 prior to being granted authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances. |
|  | If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies. |
| **Note to Auditor:**  The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R2 – Cyber Security Training Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.3 | High Impact BES Cyber Systems and their associated:   * EACMS; and * PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Require completion of the training specified in Part 2.1 at least once every 15 calendar months. | Examples of evidence may include, but are not limited to, dated individual training records. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 2.3

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify all personnel with authorized electronic access or authorized unescorted physical access to applicable Cyber Assets completed the training specified in Part 2.1 at least once every 15 calendar months. |

**[Compliance Summary:](#R2)**

|  |
| --- |
| Finding Summary:  Primary Documents Supporting Findings: |

**Auditor Notes:**

|  |
| --- |
|  |

R3 Supporting Evidence and Documentation

**R3.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-5.1 Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

**M3.** Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in CIP-004-5.1 Table R3 – Personnel Risk Assessment Program and additional evidence to demonstrate implementation of the program(s).

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R3 – Personnel Risk Assessment Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.1 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Process to confirm identity. | An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to confirm identity. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 3.1

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include a process to confirm identity. |
|  | Verify a process to confirm identity was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems. |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R3 – Personnel Risk Assessment Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.2 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:   * + 1. current residence, regardless of duration; and     2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.   If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed. | An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to perform a seven year criminal history records check. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 3.2

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include a process to perform a seven year criminal history records check that includes:   1. current residence, regardless of duration; 2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more; and 3. performing as much of the seven year criminal history records check as possible, if it is not possible to perform a full seven year criminal history records check. |
|  | Verify a process to perform a seven year criminal history records check was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to applicable Cyber Systems and:   * A full seven year criminal history records check was completed; or * A full seven year criminal history records check was not completed, the Responsible Entity completed as much of the seven year criminal history records check as possible, and documented the reason the full seven year criminal history records check was not completed. |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R3 – Personnel Risk Assessment Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.3 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Criteria or process to evaluate criminal history records checks for authorizing access. | An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to evaluate criminal history records checks. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 3.3

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include criteria or a process to evaluate criminal history records checks for authorizing access. |
|  | Verify the applicable criteria or process to evaluate criminal history records checks for authorizing access was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems. |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R3 – Personnel Risk Assessment Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.4 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3. | An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s criteria or process for verifying contractors or service vendors personnel risk assessments. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 3.4

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include criteria or a process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3. |
|  | Verify the criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3 was implemented. |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R3 – Personnel Risk Assessment Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 3.5 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years. | An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 3.5

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include a process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years. |
|  | For personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems, verify the applicable personnel risk assessment process was implemented at least once every seven years. |

**[Compliance Summary:](#R3)**

|  |
| --- |
| Finding Summary:  Primary Documents Supporting Findings: |

**Auditor Notes:**

|  |
| --- |
|  |

R4 Supporting Evidence and Documentation

**R4.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in CIP-004-5.1 Table R4 – Access Management Program*. [Violation Risk Factor: Medium*] *[Time Horizon: Operations Planning and Same Day Operations]*.

**M4.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R4 – Access Management Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 4.1 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:   * + 1. Electronic access;     2. Unescorted physical access into a Physical Security Perimeter; and     3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. | An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 4.1

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more access management programs which include a process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:   1. Electronic access; 2. unescorted physical access into a Physical Security Perimeter; and 3. access to designated storage locations, whether physical or electronic, for BES Cyber System Information. |
|  | If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies. |
|  | Verify access was authorized, based on need, for:   1. Electronic access; 2. unescorted physical access into a Physical Security Perimeter; and 3. access to designated storage locations, whether physical or electronic, for BES Cyber System Information. |
| **Note to Auditor:**  The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R4 – Access Management Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 4.2 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records. | Examples of evidence may include, but are not limited to:  • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or  • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing). |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 4.2

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more access management programs which include a process to verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records. |
|  | Verify the Responsible Entity has verified at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records. |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R4 – Access Management Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 4.3 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary. | An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:   1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 4.3

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more access management programs that, for electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary. |
|  | Verify the Responsible Entity has verified, at least once every 15 calendar months, that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct. |
|  | Verify the Responsible Entity has verified, at least once every 15 calendar months, that user accounts, user account groups, or user role categories, and their specific, associated privileges are those that the Responsible Entity determines are necessary. |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R4 – Access Management Program** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 4.4 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions. | An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:   1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 4.4

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more access management programs that verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions. |
|  | Verify the Responsible Entity has verified, at least once every 15 calendar months, that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct. |
|  | Verify the Responsible Entity has verified, at least once every 15 calendar months, that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are those that the Responsible Entity determines are necessary for performing assigned work functions. |

**[Compliance Summary:](#R4)**

|  |
| --- |
| Finding Summary:  Primary Documents Supporting Findings: |

**Auditor Notes:**

|  |
| --- |
|  |

R5 Supporting Evidence and Documentation

**R5.** Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations*

*Planning].*

**M5.** Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R5 – Access Revocation** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 5.1 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | A process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). | An example of evidence may include, but is not limited to, documentation of all of the following:   1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 5.1

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more access revocation programs that include a process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). |
|  | Verify the Responsible Entity has:   1. initiated removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action; and 2. completed the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). |
| **Note to Auditor:**  Removal of the ability for access does not necessarily require removal or disabling of the individual’s accounts. The ability for access may be removed by disabling the individual’s network access, confiscation of a badge, or other suitable means. Removal of Interactive Remote Access may be accomplished, for example, by disabling the individual’s multi-factor authentication. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R5 – Access Revocation** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 5.2 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access. | An example of evidence may include, but is not limited to, documentation of all of the following:  1. Dated workflow or sign-off form showing a review of logical and physical access; and  2. Logs or other demonstration  showing such persons no longer have access that the Responsible Entity determines is not necessary. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 5.2

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more access revocation programs for reassignments or transfers to revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access. |
|  | Verify the Responsible Entity has, for reassignments or transfers, revoked the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access. |
| **Note to Auditor:**  Revocation of access does not necessarily require removal of the individual’s accounts. The account may be disabled in lieu of removal. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R5 – Access Revocation** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 5.3 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:   1. EACMS; and 2. PACS | For termination actions, revoke the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action. | An example of evidence may include, but is not limited to, workflow or sign- off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 5.3

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more access revocation programs for termination actions to revoke the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5, Part 5.1), by the end of the next calendar day following the effective date of the termination action. |
|  | Verify the Responsible Entity has, for termination actions, revoked the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action. |
| **Notes to Auditor:**   1. If the access was already revoked under the actions taken for Requirement R5, Part 5.1, no further action is needed. 2. Revocation of access does not necessarily require removal or disabling of the individual’s accounts. The ability for access may be removed by disabling the individual’s network access, confiscation of a badge, or other suitable means. 3. Removal of Interactive Remote Access may be accomplished, for example, by disabling the individual’s multi-factor authentication. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-004-5.1 Table R5 – Access Revocation** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 5.4 | High Impact BES Cyber Systems and their associated:   * EACMS | For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action. | An example of evidence may include, but is not limited to, workflow or sign- off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 5.4

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more access revocation programs for termination actions to revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action. |
|  | Verify the Responsible Entity, for termination actions, has revoked the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action. |
| **Note to Auditor:**  Revocation of access does not necessarily require removal of the individual’s accounts. The account may be disabled in lieu of removal. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **CIP-0046 Table R5 – Access Revocation** | | | |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 5.5 | High Impact BES Cyber Systems and their associated:   * EACMS | For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.  If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances. | Examples of evidence may include, but are not limited to:   * Workflow or sign-off form showing password reset within 30 calendar days of the termination; * Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or * Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance. |

**Registered Entity Response (Required):**

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found. | | | | | |
| **File Name** | **Document Title** | **Revision or Version** | **Document Date** | **Relevant Page(s) or Section(s)** | **Description of Applicability of Document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Audit Team Evidence Reviewed (This section to be completed by the Compliance Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 5.5

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more access revocation programs for termination actions to change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.  The documented process(es) may include provisions for the Responsible Entity to determine and document that extenuating operating circumstances require a longer time period, and may change the password(s) within 10 calendar days following the end of the operating circumstances. |
|  | If extenuating operating circumstances are invoked, verify the circumstances are documented and include a specific end date. |
|  | For termination actions that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 30 calendar days of the termination action. |
|  | For termination actions that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 10 calendar days following the end of the extenuating operating circumstances. |
|  | For reassignments or transfers that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 30 calendar days of the date that the Responsible Entity determines the individual no longer requires retention of the access. |
|  | For reassignments or transfers that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 10 calendar days following the end of the extenuating operating circumstances. |

**[Compliance Summary:](#R5)**

|  |
| --- |
| Finding Summary:  Primary Documents Supporting Findings: |

**Auditor Notes:**

|  |
| --- |
|  |

**Revision History for RSAW**

|  |  |  |
| --- | --- | --- |
| **Date** | **Reviewer(s)** | **Revision Description** |
| 3/4/2016 | Jennifer Salisbury, WECC  Julie Blair, WECC  WECC CIP SME | Intial version |
|  |  |  |
|  |  |  |
|  |  |  |