

**Reliability Standard Audit Worksheet for British Columbia**

# CIP-003-5 – Cyber Security — Security Management Controls

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, GOPTO, TOP |
| [R3](#R3_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |
| [R4](#R4_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, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

**1.1** Personnel & training (CIP-004);

**1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

**1.3** Physical security of BES Cyber Systems (CIP-006);

**1.4** System security management (CIP-007);

**1.5** Incident reporting and response planning (CIP-008);

**1.6** Recovery plans for BES Cyber Systems (CIP-009);

**1.7** Configuration change management and vulnerability assessments (CIP-010);

**1.8** Information protection (CIP-011); and

**1.9** Declaring and responding to CIP Exceptional Circumstances.

**M1.** Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

**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

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

|  |  |
| --- | --- |
|  | For its high impact and medium impact BES Cyber Systems, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics:   1. Personnel and training (CIP-004); 2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access; 3. Physical security of BES Cyber Systems (CIP-006); 4. System security management (CIP-007); 5. Incident reporting and response planning (CIP-008); 6. Recovery plans for BES Cyber Systems (CIP-009); 7. Configuration change management and vulnerability assessments (CIP-010); 8. Information protection (CIP-011); and 9. Declaring and responding to CIP Exceptional Circumstances. |
|  | For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics:   1. Cyber security awareness; 2. Physical security controls; 3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and 4. Cyber Security Incident response. |
|  | Verify each policy used to meet this Requirement has been reviewed at least once every 15 calendar months. |
|  | Verify the CIP Senior Manager has approved each policy used to meet this Requirement at least once every 15 calendar months. |
| **Note to Auditor:**  Per Attachment 1, “Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.” | |

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

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

**Auditor Notes:**

|  |
| --- |
|  |

**R2 Supporting Evidence and Documentation**

**R2**. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

**2.1** Cyber security awareness;

**2.2** Physical security controls;

**2.3** Electronic access controls for external routable protocol connections and Dial-up

Connectivity; and

**2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their

BES Cyber Assets is not required.

**M2.** Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

**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

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

|  |  |
| --- | --- |
|  | For each asset or group of assets containing low impact BES Cyber Systems, verify that the Responsible Entity has documented one or more cyber security plan(s), as specified in Attachment 1, for its low impact BES Cyber Systems that include:   1. Cyber security awareness; 2. physical security controls; 3. electronic access controls; and 4. Cyber Security Incident response |
|  | For each asset or group of assets containing low impact BES Cyber Systems, verify that the Responsible Entity has reinforced cyber security awareness of its cyber security practices (which may include associated physical security practices) at least once every 15 calendar months. |
|  | For each asset or group of assets containing low impact BES Cyber Systems, verify that the Responsible Entity has implemented physical access controls, based on need as determined by the Responsible Entity, to control physical access to:   1. The asset or the locations of the low impact BES Cyber Systems within the asset; and 2. the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any. |
|  | For each asset or group of assets containing low impact BES Cyber Systems, does the Responsible Entity have any Low Impact External Routable Connectivity (LERC)?   * If yes, verify that the Responsible Entity implemented a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access. * If no, verify that LERC does not exist. |
|  | For each asset or group of assets containing low impact BES Cyber Systems, verify that the Responsible Entity has implemented authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability. |
|  | For each asset or group of assets containing low impact BES Cyber Systems, verify that the Responsible Entity has one or more Cyber Security Incident response plan(s) that includes:   1. Identification, classification, and response to Cyber Security Incidents; 2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law; 3. Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals; 4. Incident handling for Cyber Security Incidents; 5. Testing each Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and 6. Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident. |
|  | For each asset or group of assets containing low impact BES Cyber Systems, if the Responsible Entity responded to a Cyber Security Incident, verify the Responsible Entity implemented the Cyber Security Incident response plan. |
|  | Verify the Responsible Entity tested each Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident. |
|  | Verify the Responsible Entity updated each Cyber Security Incident response plan, if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident. |

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

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

**Auditor Notes:**

|  |
| --- |
|  |

**R3 Supporting Evidence and Documentation**

**R3.** Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

**M3.** An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

**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

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

|  |  |
| --- | --- |
|  | Verify the CIP Senior Manager has been identified by name. |
|  | Verify that any changes made to the CIP Senior Manager were dated and documented within 30 calendar days of the change. |
|  | Verify the CIP Senior Manager is a single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the CIP Reliability Standards for BC, CIP-002 through CIP-011. |

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

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

**Auditor Notes:**

|  |
| --- |
|  |

**R4 Supporting Evidence and Documentation**

**R4.** The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

**M4.** An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

**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

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

|  |  |
| --- | --- |
|  | Verify that the Responsible Entity has documented a process to delegate authority, unless no delegations are used. |
|  | Verify that all delegates have been identified by name or title. |
|  | Verify that the delegation of authority includes the specific action delegated. |
|  | Verify specific actions delegated by the CIP Senior Manager are allowed by the CIP Reliablility Standards for BC. |
|  | Verify that the dates for all delegations have been recorded. |
|  | Verify that the CIP Senior Manager approved all delegations. |
|  | Verify that any changes made to delegations were dated and documented within 30 days of the change. |
| **Note to Auditor:**  Delegations of the CIP Senior Manager’s authority are permitted for the required approvals in CIP-002-5.1, Requirement R2 and CIP-007-6, Requirement R2, Part 2.4. | |

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

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

**Auditor Notes:**

|  |
| --- |
|  |

**Revision History for RSAW**

|  |  |  |
| --- | --- | --- |
| **Date** | **Reviewer(s)** | **Revision Description** |
| 2/24/2016 | Jennifer Salisbury, WECC  Julie Blair, WECC  WECC CIP SME | Intial version |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |