

**Reliability Standard Audit Worksheet for British Columbia**

# CIP-011-1 – Cyber Security – Information Protection

# 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 |

|  |  |
| --- | --- |
| 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, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

**M1.** Evidence for the information protection program must include the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table*.*

| **CIP-011-1 Table R1 – Information Protection** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.1 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS | Method(s) to identify information that meets the definition of BES Cyber System Information. | Examples of acceptable evidence include, but are not limited to:   * Documented method to identify BES Cyber System Information from entity’s information protection program; or * Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity’s information protection program; or * Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or * Repository or electronic and physical location designated for housing BES Cyber System Information in the entity’s information protection program. |

**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 information protection programs that have method(s) to identify information that meets the definition of BES Cyber System Information. |
|  | Verify the Responsible Entity has implemented the method(s) to identify information that meets the definition of BES Cyber System Information. |

| **CIP-011-1 Table R1 – Cyber Security Incident Response Plan Specifications** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.2 | High Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS   Medium Impact BES Cyber Systems and their associated:   1. EACMS; and 2. PACS | Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. | Examples of acceptable evidence include, but are not limited to:   * Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or * Records indicating that BES Cyber System Information is handled in a manner consistent with the entity’s documented procedure(s). |

**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 1.2

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

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more information protection programs that include procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. |
|  | Verify the Responsible Entity has implemented the procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. |

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

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

**Auditor Notes:**

|  |
| --- |
|  |

**R2 Supporting Evidence and Documentation**

**R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

**M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

| **CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.1 | High Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA   Medium Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA | Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. | Examples of acceptable evidence include, but are not limited to:   * Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or * Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of 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 2.1

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

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes to take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media, prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column). |
|  | Verify that prior to the release for reuse of Cyber Assets of Applicable Systems that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity has taken action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. |

| **CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal** | | | |
| --- | --- | --- | --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 2.2 | High Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA   Medium Impact BES Cyber Systems and their associated:   1. EACMS; 2. PACS; and 3. PCA | Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media. | Examples of acceptable evidence include, but are not limited to:   * Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or * Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset. |

**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 the Responsible Entity has documented one or more processes to take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media, prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information. |
|  | Verify that, prior to the disposal of Cyber Assets of Applicable Systems that contain BES Cyber System Information, the Responsible Entity has taken action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroyed the data storage media. |

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

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

**Auditor Notes:**

|  |
| --- |
|  |

**Revision History for RSAW**

|  |  |  |
| --- | --- | --- |
| **Date** | **Reviewer(s)** | **Revision Description** |
| 3/7/2016 | Jennifer Salisbury, WECC  Julie Blair, WECC  WECC CIP SME | Intial version |
|  |  |  |
|  |  |  |