**Formulaire d’audit de la norme de fiabilité au Québec**

**CIP-004-6 — Cybersécurité - Personnel et formation**

***Cette section doit être complétée par le NPCC.***

|  |  |
| --- | --- |
| **Numéro de l’audit:** | NPCC-NIRnnnn-YYYYMMDD |
| **Entité visée:** | Nom de l’entité visée |
| **Numéro d’identification à la Régie:** | NIRnnnn |
| **Responsable des mesures pour assurer la conformité:** | Régie de l’énergie |
| **Date(s)**[[1]](#footnote-1) **d’évaluation de la conformité:** | Du jour mois année au jour mois année |
| **Processus de surveillance de la conformité:** | [Audit sur place | Audit hors site | Contrôle ponctuel] |
| **Noms des auditeurs:** | Fournis par le NPCC |

Applicabilité des exigences:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **BA** | **DP** | **GO** | **GOP** | **LSE** | **PA** | **RC** | **RP** | **TO** | **TOP** | **TP** | **TSP** |
| **E1** | **X** | **X** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |
| **E2** | **X** | **X** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |
| **E3** | **X** | **X** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |
| **E4** | **X** | **X** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |
| **E5** | **X** | **X** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |

**Légende:**

|  |  |
| --- | --- |
| Texte avec fond bleu: | Texte figé – ne pas modifier |
| Zone d’entrée de texte avec fond vert: | Information fournie par l’entité |
| Zone d’entrée de texte avec fond blanc: | Information fournie par l’auditeur |

**Clause de non-responsabilité**

Ce formulaire d’audit de la norme de fiabilité au Québec (formulaire) a été conçu pour faciliter l’évaluation, par le NPCC, de la conformité à cette norme de fiabilité et son annexe (l’Annexe) d’une entité visée au Québec. Ce formulaire contient toutes les questions et tous les sujets pertinents du formulaire correspondant de la NERC utilisé aux États-Unis. Le texte du formulaire est adapté aux versions spécifiques de chaque norme de fiabilité. Les entités qui utilisent ce formulaire devraient choisir la version du formulaire qui s’applique à la norme de fiabilité qui est évaluée. Bien que l’information contenue dans ce formulaire dévoile en partie la méthodologie que le NPCC a choisie pour évaluer la conformité aux exigences de la norme de fiabilité, ce document ne doit pas remplacer la norme de fiabilité ou ne doit pas être vu comme un ajout d’exigences à la norme de fiabilité. Dans tous les cas, l’entité régionale doit se baser sur le texte de la norme de fiabilité elle-même et non sur le texte de ce formulaire, pour déterminer la conformité à la norme de fiabilité. Les normes de fiabilité peuvent être consultées [sur le site internet de la Régie](http://www.regie-energie.qc.ca/audiences/NormesFiabiliteTransportElectricite/NormesFiabilite.html). Par ailleurs, les normes de fiabilité sont fréquemment mises à jour et il se peut que ce formulaire ne soit pas mis à jour à la même fréquence. Par conséquent, il est impératif que les entités visées considèrent ce formulaire comme un document de référence seulement et non comme un suppléant ou remplaçant de la norme de fiabilité. Il est de la responsabilité de l’entité visée de vérifier si elle est conforme à la dernière version approuvée, par l’autorité gouvernementale applicable, de la norme de fiabilité, en fonction de son inscription [au registre des entités](http://www.regie-energie.qc.ca/audiences/NormesFiabiliteTransportElectricite/RegistreEntites.html).

Ce formulaire fournit, à titre d’information seulement, une liste non-exclusive d’exemples de types de pièces justificatives qu’une entité visée pourrait devoir fournir ou pourrait être demandée de fournir pour démontrer la conformité à la norme de fiabilité. Les pièces justificatives soumises par l’entité visée pour répondre aux exemples de ce formulaire n’assurent pas nécessairement la conformité à la norme de fiabilité, et le NPCC se réserve le droit de demander des pièces justificatives additionnelles, non contenue dans le formulaire, de la part de l’entité visée.

Constats

**(Cette section doit être complétée par le NPCC)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Exig.** | **Constat** | **Résumé et documentation** | **Fonctions surveillées** |
| **E1** |  |  |  |
| A1.1 |  |  |  |
| **E2** |  |  |  |
| A2.1 |  |  |  |
| A2.2 |  |  |  |
| A2.3 |  |  |  |
| **E3** |  |  |  |
| A3.1 |  |  |  |
| A3.2 |  |  |  |
| A3.3 |  |  |  |
| A3.4 |  |  |  |
| A3.5 |  |  |  |
| **E4** |  |  |  |
| A4.1 |  |  |  |
| A4.2 |  |  |  |
| A4.3 |  |  |  |
| A4.4 |  |  |  |
| **E5** |  |  |  |
| A5.1 |  |  |  |
| A5.2 |  |  |  |
| A5.3 |  |  |  |
| A5.4 |  |  |  |
| A5.5 |  |  |  |

|  |  |
| --- | --- |
| **Exig.** | **Sujets de préoccupation** |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| **Exig.** | **Recommandations** |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| **Exig.** | **Observations positives** |
|  |  |
|  |  |
|  |  |

**Experts en la matière**

Identifier le ou les experts en la matière, responsables de la norme de fiabilité.

**Réponse de l’entité visée (Requise; Veuillez insérez des lignes supplémentaires, si nécessaire) :**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nom de l’expert en la matière** | **Titre** | **Organisation** | **Exigence(s)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**E1 Documentation et pièces justificatives à l’appui**

1. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-004-6) – Programme de sensibilisation à la sécurité. *[Facteur de risque de non-conformité : faible] [Horizon : planification de l’exploitation]*
2. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-004-6) – Programme de sensibilisation à la sécurité ; ainsi que des pièces justificatives additionnelles pour démontrer la mise en œuvre tel que décrit dans la colonne Mesures du tableau.

**E1 Alinéa 1.1**

| **Tableau E1 (CIP-004-6) – Programme de sensibilisation à la sécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.1 | *Systèmes électroniques BES* à impact élevé.  *Systèmes électroniques BES* à impact moyen. | Une sensibilisation à la sécurité qui, au moins une fois par trimestre civil, rappelle les pratiques de cybersécurité (pouvant inclure les pratiques de sécurité physique associées) au personnel de l’entité responsable qui a un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *systèmes électroniques BES*. | Exemple non limitatif de pièces justificatives : des documents attestant que le rappel trimestriel a été fait. Exemples non limitatifs de pièces justificatives du rappel : des copies datées de l’information utilisée pour rappeler les pratiques de sécurité et des pièces justificatives de distribution, notamment :   * communications ciblées (p. ex., courriels, notes de service, formation en ligne, etc.) ; * communications générales (p. ex., affiches, intranet, brochures, etc.) ; ou * rappels et soutien de la direction (p. ex., présentations, réunions, etc.). |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E1, alinéa 1.1**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus incluant une sensibilisation à la sécurité qui, au moins une fois par trimestre civil, rappelle les pratiques de cybersécurité (pouvant inclure les pratiques de sécurité physique associées) au personnel de l’entité responsable qui a un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *systèmes électroniques BES*. |
|  | Vérifier que l’entité responsable a rappelé la sensibilisation à la sécurité au moins une fois par trimestre civil. |
|  | Vérifier que le rappel en ce qui a trait à la sensibilisation à la sécurité comprend :   * un rappel des pratiques de cybersécurité, ou; * un rappel des pratiques de sécurité physique associées à la cybersécurité. |
|  | Vérifier que la sensibilisation à la sécurité a été rappelée au personnel de l’entité responsable qui a un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *systèmes électroniques BES*. |
| **Notes pour l’auditeur:**  L’entité responsable n’est pas tenue de documenter que chaque rappel trimestriel a été fait à chacun des membres de son personnel autorisé. L’entité responsable est plutôt tenue de démontrer que le rappel en ce qui a trait à la sensibilisation à la sécurité a été communiqué à son personnel autorisé dans son ensemble, pas nécessairement individuellement. | |

**Notes des auditeurs:**

**E2 Documentation et pièces justificatives à l’appui**

1. Chaque entité responsable doit mettre en œuvre un ou des programmes de formation sur la cybersécurité axée sur les rôles, les fonctions ou les responsabilités de chacun, qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité. *[Facteur de risque de non-conformité : faible] [Horizon : planification de l’exploitation]*
2. Les pièces justificatives doivent comprendre les programmes de formation qui couvrent tous les alinéas applicables du tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité ; d’autres pièces justificatives doivent attester la mise en œuvre des programmes.

**E2 Alinéa 2.1**

| **Tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.1 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les *PACS* associés.   *Systèmes électroniques BES* à impact moyen à connectivité externe routable et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Formation portant sur :   * + 1. les politiques de cybersécurité ;     2. le contrôle des accès physiques ;     3. le contrôle des accès électroniques ;     4. le programme de contrôle des visiteurs ;     5. la gestion et le stockage de l’information des *systèmes électroniques BES* ;     6. la détection des *incidents de cybersécurité* et l’envoi des avis initiaux conformément au plan d’intervention en cas d’incident de l’entité;     7. les plans de rétablissement des *systèmes électroniques BES* ;     8. l’intervention en cas d’*incident* *de cybersécurité* ; et     9. les risques pour la cybersécurité associés à l’interconnectabilité et à l’interopérabilité des *systèmes électroniques BES* avec d’autres *actifs électroniques*, y compris des *actifs électroniques* *transitoires* et des *supports de stockage amovibles*. | Exemples non limitatifs de pièces justificatives : matériel de formation comme des présentations PowerPoint, des notes à l’intention des formateurs ou des étudiants, ou des documents de cours. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E2, alinéa 2.1**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que le ou les programmes de formation sur la cybersécurité couvrent les alinéas suivants :   * + 1. les politiques de cybersécurité ;     2. le contrôle des accès physiques ;     3. le contrôle des accès électroniques ;     4. le programme de contrôle des visiteurs ;     5. la gestion et le stockage de l’information des *systèmes électroniques BES*;     6. la détection des *incidents de cybersécurité* et l’envoi des avis initiaux conformément au plan d’intervention en cas d’incident de l’entité ;     7. les plans de rétablissement des *systèmes électroniques BES*;     8. l’intervention en cas d’*incident de cybersécurité*; et     9. les risques pour la cybersécurité associés à l’interconnectabilité et à l’interopérabilité des *systèmes électroniques BES* avec d’autres *actifs électroniques*, y compris des *actifs électroniques transitoires* et des *supports de stockage amovibles*. |
|  | Vérifier que le contenu du ou des programmes de formation de l’entité responsable soit approprié quant aux rôles, fonctions ou responsabilités de chacun. |
| **Notes pour l’auditeur:**   1. Le ou les programmes de formation sur la cybersécurité doivent collectivement inclure chacun des neuf éléments de formation. 2. Il n’est pas nécessaire d’inclure chacun des neuf éléments de formation à la formation de chaque rôle, fonction ou responsabilité. 3. Chaque rôle, fonction ou responsabilité doit recevoir une formation qui couvre tous les éléments de formation pertinents. | |

**Notes des auditeurs:**

**E2 Alinéa 2.2**

| **Tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.2 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les *PACS* associés.   *Systèmes électroniques BES* à impact moyen à connectivité externe routable et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Exiger que soit suivie au complet la formation énoncée à l’alinéa 2.1 avant que soit accordé un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *actifs électroniques* visés, sauf dans des *circonstances CIP exceptionnelles*. | Exemples non limitatifs de pièces justificatives : registres de formation et documents attestant l’invocation de *circonstances CIP exceptionnelles*. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E2, alinéa 2.2**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’ensemble du personnel a suivi au complet la formation énoncée à l’alinéa 2.1 avant que soit accordé un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *actifs électroniques* visés, sauf dans des *circonstances CIP exceptionnelles*. |
|  | Si l’entité responsable a déclaré ou répondu à des *circonstances CIP exceptionnelles*, vérifier que l’entité responsable s’est conformée aux politiques de cybersécurité applicables. |
| **Notes pour l’auditeur:**  L'entité responsable peut faire référence à un ensemble distinct de documents pour démontrer sa conformité à toutes les exigences touchées par les *circonstances CIP exceptionnelles*. | |

**Notes des auditeurs:**

**E2 Alinéa 2.3**

| **Tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.3 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les *PACS* associés.   *Systèmes électroniques BES* à impact moyen à connectivité externe routable et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Exiger que la formation énoncée à l’alinéa 2.1 soit suivie au complet au moins une fois tous les 15 mois civils. | Exemple non limitatif de pièces justificatives : registres de formation individuels datés. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E2, alinéa 2.3**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’ensemble du personnel avec des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement à des *actifs électroniques* visés, a suivi au complet la formation énoncée à l’alinéa 2.1 au moins une fois tous les 15 mois civils. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E3 Documentation et pièces justificatives à l’appui**

1. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés d’évaluation des risques liés au personnel en vue de l’octroi ou du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement à des *systèmes électroniques BES* et qui, collectivement, couvrent tous les parties alinéas applicables du tableau E3 (CIP-004-6) – Programme d’évaluation des risques liés au personnel. *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l’exploitation]*
2. Les pièces justificatives doivent comprendre le ou les programmes documentés d’évaluation des risques liés au personnel qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-004-6) – Programme d’évaluation des risques liés au personnel ; d’autres pièces justificatives doivent attester la mise en œuvre du ou des programmes.

**E3 Alinéa 3.1**

| **Tableau E3 (CIP-004-6) – Programme d’évaluation des risques liés au personnel** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.1 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Processus de confirmation de l’identité. | Exemple non limitatif de pièces justificatives : documents attestant le processus suivi par l’entité responsable pour confirmer l’identité. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E3, alinéa 3.1**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes d’évaluation des risques liés au personnel en vue de l’octroi ou du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement à des *systèmes électroniques BES*, qui comprennent un processus de confirmation de l’identité. |
|  | Vérifier qu’un processus de confirmation de l’identité a été mis en œuvre pour le personnel qui a un accès électronique autorisé et/ou un accès physique autorisé sans accompagnement aux systèmes visés. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E3 Alinéa 3.2**

| **Tableau E3 (CIP-004-6) – Programme d’évaluation des risques liés au personnel** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.2 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Processus de vérification des antécédents judiciaires sur les sept années précédentes dans le cadre de chaque évaluation des risques liés au personnel, qui comprend :   * + 1. le lieu où réside actuellement la personne, peu importe depuis combien de temps ; et     2. les autres endroits où, au cours des sept années précédant la date de vérification des antécédents judiciaires, la personne a résidé pendant au moins six mois consécutifs.   S’il est impossible de mener une vérification complète des antécédents judiciaires sur les sept années précédentes, pousser la vérification le plus loin possible et consigner les motifs pour lesquels la vérification complète sur cette période n’a pu se faire. | Exemple non limitatif de pièces justificatives : documents attestant le processus suivi par l’entité responsable pour vérifier les antécédents criminels sur les sept dernières années. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E3, alinéa 3.2**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes d’évaluation des risques liés au personnel en vue de l’octroi ou du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement à des *systèmes électroniques BES*, y compris un processus de vérification des antécédents judiciaires sur les sept années précédentes qui comprend :   1. le lieu où réside actuellement la personne, peu importe depuis combien de temps; 2. les autres endroits où, au cours des sept années précédant la date de vérification des antécédents judiciaires, la personne a résidé pendant au moins six mois consécutifs; et 3. S’il est impossible de mener une vérification complète des antécédents judiciaires sur les sept années précédentes, pousser la vérification le plus loin possible. |
|  | Vérifier qu’un processus de vérification des antécédents judiciaires sur les sept années précédentes a été mis en œuvre pour le personnel qui a un accès électronique autorisé et/ou un accès physique autorisé sans accompagnement à des *systèmes électroniques* visés et vérifier que :   * une vérification complète des antécédents judiciaires sur les sept années précédentes a été effectuée; ou * une vérification complète des antécédents judiciaires sur les sept années précédente n’a pas été effectuée, mais l’entité responsable a poussé la vérification le plus loin possible et a consigné les motifs pour lesquels la vérification complète sur cette période n’a pu se faire. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E3 Alinéa 3.3**

| **Tableau E3 (CIP-004-6) – Programme d’évaluation des risques liés au personnel** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.3 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Critères ou processus pour évaluer les résultats de la vérification des antécédents judiciaires en vue d’autoriser un accès. | Exemple non limitatif de pièces justificatives : documents attestant le processus de l’entité responsable pour évaluer les résultats des vérifications des antécédents judiciaires. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E3, alinéa 3.3**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes d’évaluation des risques liés au personnel en vue de l’octroi ou du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement à des *systèmes électroniques BES*, y compris des critères ou un processus pour évaluer les résultats de la vérification des antécédents judiciaires en vue d’autoriser un accès. |
|  | Vérifier que les critères ou processus pour évaluer les résultats de la vérification des antécédents judiciaires en vue d’autoriser un accès ont été mis en œuvre pour le personnel avec des accès électroniques autorisés et/ou des accès physiques autorisés sans accompagnement aux systèmesvisés. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E3 Alinéa 3.4**

| **Tableau E3 (CIP-004-6) – Programme d’évaluation des risques liés au personnel** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.4 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Critères ou processus pour vérifier que les évaluations des risques liés au personnel dont les contractuels et les fournisseurs de services doivent faire l’objet sont menées conformément aux alinéas 3.1 à 3.3. | Exemples non limitatifs de pièces justificatives : documents attestant les critères ou le processus de l’entité responsable pour vérifier les évaluations des risques liés au personnel pour les contractuels et les fournisseurs de services. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E3, alinéa 3.4**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes d’évaluation des risques liés au personnel en vue de l’octroi ou du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement à des *systèmes électroniques BES*, y compris des critères ou un processus pour vérifier que les évaluations des risques liés au personnel dont les contractuels et les fournisseurs de services doivent faire l’objet sont menées conformément aux alinéas 3.1 à 3.3. |
|  | Vérifier la mise en œuvre des critères ou du processus pour vérifier que les évaluations des risques liés au personnel dont les contractuels et les fournisseurs de services doivent faire l’objet sont menées conformément aux alinéas 3.1 à 3.3. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E3 Alinéa 3.5**

| **Tableau E3 (CIP-004-6) – Programme d’évaluation des risques liés au personnel** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.5 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Processus permettant de s’assurer que les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement ont fait l’objet d’une évaluation des risques liés au personnel conformément aux alinéas 3.1 à 3.4 au cours des sept dernières années. | Exemples non limitatifs de pièces justificatives : documents attestant le processus suivi par l’entité responsable pour s’assurer que les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement ont fait l’objet d’une évaluation des risques liés au personnel au cours des sept dernières années. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E3, alinéa 3.5**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes d’évaluation des risques liés au personnel en vue de l’octroi ou du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement à des *systèmes électroniques BES*, y compris un processus permettant de s’assurer que les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement ont fait l’objet d’une évaluation des risques liés au personnel conformément aux alinéas 3.1 à 3.4 au cours des sept dernières années. |
|  | Pour le personnel ayant des accès électroniques autorisés et/ou des accès physiques autorisés sans accompagnement à des systèmesvisés, vérifier que le processus correspondant d’évaluation des risques liés au personnel a été mis en œuvre au moins une fois toutes les sept années civiles. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E4 Documentation et pièces justificatives à l’appui**

1. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de gestion des accès qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-004-6) – Programme de gestion des accès. *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l’exploitation et exploitation le même jour]*
2. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-004-6) – Programme de gestion des accès ; d’autres pièces justificatives doivent attester la mise en œuvre des mesures du programme de gestion des accès selon la colonne Mesures du tableau.

**E4 Alinéa 4.1**

| **Tableau E4 (CIP-004-6) – Programme de gestion des accès** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.1 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Processus d’autorisation selon le besoin déterminé par l’entité responsable, sauf dans des *circonstances CIP exceptionnelles* :   * + 1. de l’accès électronique ;     2. de l’accès physique sans accompagnement dans un *périmètre de sécurité physique*; et     3. de l’accès à des emplacements de stockage (physiques ou électroniques) désignés pour l’information de *système électronique BES*. | Exemples non limitatifs de pièces justificatives : documents datés attestant le processus suivi pour autoriser un accès électronique, un accès physique sans accompagnement à un *périmètre de sécurité physique* et un accès à des emplacements de stockage (physiques ou électroniques) désignés pour l’information de *système électronique BES*. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E4, alinéa 4.1**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes de gestion des accès incluant un processus d’autorisation, selon le besoin déterminé par l’entité responsable, sauf dans des *circonstances CIP exceptionnelles*:   1. de l’accès électronique ; 2. de l’accès physique sans accompagnement dans un *périmètre de sécurité physique* ; et 3. de l’accès à des emplacements de stockage (physiques ou électroniques) désignés pour l’information de *système électronique BES*. |
|  | Si l’entité responsable a déclaré et répondu à des *circonstances CIP exceptionnelles*, vérifier que l’entité responsable s’est conformée aux politiques de cybersécurité applicables. |
|  | Vérifier que l’accès a été autorisé, selon le besoin, pour :   1. l’accès électronique ; 2. l’accès physique sans accompagnement dans un *périmètre de sécurité physique* ; et 3. l’accès à des emplacements de stockage (physiques ou électroniques) désignés pour l’information de *système électronique BES*. |
| **Notes pour l’auditeur:**  L’entité responsable peut faire référence à d’autres documents que ceux demandés à la mesure M4.1 pour démontrer sa conformité à toute exigence touchée par des *circonstances CIP exceptionnelles*. | |

**Notes des auditeurs:**

**E4 Alinéa 4.2**

| **Tableau E4 (CIP-004-6) – Programme de gestion des accès** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.2 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Vérifier, au moins une fois par trimestre civil, que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d’accès autorisé. | Exemples non limitatifs de pièces justificatives :   * documents datés attestant une comparaison entre la liste automatisée des personnes pour lesquelles on a autorisé l’accès (base de données des activités de fourniture) et la liste automatisée des personnes auxquelles on a fourni un accès (liste des comptes utilisateurs) ; ou * documents datés attestant une comparaison entre la liste des personnes pour lesquelles on a autorisé l’accès (formulaires d’autorisation) et la liste des personnes auxquelles on a fourni un accès (formulaires de fourniture d’accès ou liste des comptes partagés). |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E4, alinéa 4.2**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes de gestion des accès incluant un processus utilisé pour vérifier, au moins une fois par trimestre civil, que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d’accès autorisé. |
|  | Vérifier que l’entité responsable a vérifié, au moins une fois par trimestre civil, que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d’accès autorisé. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E4 Alinéa 4.3**

| **Tableau E4 (CIP-004-6) – Programme de gestion des accès** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.3 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Dans le cas des accès électroniques, vérifier, au moins une fois tous les 15 mois civils, que tous les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d’utilisateur, ainsi que leurs droits d’accès respectifs, sont correctement attribués et qu’ils sont ceux jugés nécessaires par l’entité responsable. | Exemples non limitatifs de pièces justificatives : documentation de l’examen, y compris tous les éléments suivants :   1. liste datée de tous les comptes ou groupes de comptes ou rôles au sein du système ; 2. description sommaire des droits d’accès associés à chaque groupe ou rôle ; 3. comptes attribués au groupe ou au rôle ; et 4. pièce justificative datée attestant qu’on a vérifié que les droits d’accès du groupe sont autorisés et qu’ils correspondent aux fonctions de toute personne à qui ils sont attribués. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E4, alinéa 4.3**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes de gestion des accès qui, pour les accès électroniques, vérifient, au moins une fois tous les 15 mois civils, que tous les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d’utilisateur, ainsi que leurs droits d’accès respectifs, sont correctement attribués et qu’ils sont ceux jugés nécessaires par l’entité responsable. |
|  | Vérifier que l’entité responsable a vérifié, au moins une fois tous les 15 mois civils, que tous les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d’utilisateur, ainsi que leurs droits d’accès respectifs, sont correctement attribués. |
|  | Vérifier que l’entité responsable a vérifié, au moins une fois tous les 15 mois civils, que tous les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d’utilisateur, ainsi que leurs droits d’accès respectifs, sont ceux jugés nécessaires par l’entité responsable. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E4 Alinéa 4.4**

| **Tableau E4 (CIP-004-6) – Programme de gestion des accès** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.4 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Vérifier, au moins une fois tous les 15 mois civils, que les accès aux emplacements de stockage (physiques ou électroniques) désignés pour l’information de *système électronique BES* sont correctement attribués et qu’ils correspondent à ce que l’entité responsable juge nécessaire pour les tâches à accomplir. | Exemples non limitatifs de pièces justificatives : documentation de l’examen, y compris tous les éléments suivants :   1. liste datée des autorisations d’accès à l’information de *système électronique BES* ; 2. droits d’accès associés aux autorisations ; et 3. Pièce justificative datée attestant qu’on s’est assuré que les autorisations et les droits d’accès sont correctement attribués et qu’ils correspondent au minimum nécessaire pour les tâches à accomplir. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E4, alinéa 4.4**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes de gestion des accès utilisés pour vérifier, au moins une fois tous les 15 mois civils, que les accès aux emplacements de stockage (physiques ou électroniques) désignés pour l’information de *système électronique BES* sont correctement attribués et qu’ils correspondent à ce que l’entité responsable juge nécessaire pour les tâches à accomplir. |
|  | Vérifier que l’entité responsable a vérifié, au moins une fois tous les 15 mois civils, que les accès aux emplacements de stockage (physiques ou électroniques) désignés pour l’information de *système électronique BES* sont correctement attribués. |
|  | Vérifier que l’entité responsable a vérifié, au moins une fois tous les 15 mois civils, que les accès aux emplacements de stockage (physiques ou électroniques) désignés pour l’information de *système électronique BES* correspondent à ce que l’entité responsable juge nécessaire pour les tâches à accomplir. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E5 Documentation et pièces justificatives à l’appui**

1. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de révocation d’accès qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-004-6) – Révocation d’accès. *[Facteur de risque de non-conformité : moyen] [Horizon : exploitation le même jour et planification de l’exploitation]*
2. Les pièces justificatives doivent comprendre chacun des programmes documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-004-6) – Révocation d’accès ; d’autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

**E5 Alinéa 5.1**

| **Tableau E5 (CIP-004-6) – Révocation d’accèes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.1 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Processus déclenchant le retrait à une personne de la possibilité d’accès physique sans accompagnement et d’*accès distant interactif* lors de son départ et menant à bien ce processus dans un délai de 24 heures suivant le départ. (Le retrait de la possibilité d’accès peut différer de la suppression, de la désactivation, de la révocation ou du retrait de tous les droits d’accès.) | Exemples non limitatifs de pièces justificatives :   1. formulaire d’activité ou d’approbation daté qui confirme le retrait d’accès associé au départ ; et 2. journaux ou autres pièces justificatives attestant que la personne ne dispose plus d’un accès. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E4, alinéa 5.1**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes de révocation des accès incluant un processus permettant d’initier le retrait d’accès physiques sans accompagnement et d’*accès distant interactif* d’une personne lors de son départ et menant à bien ce processus dans un délai de 24 heures suivant le départ (le retrait d’accès peut différer de la suppression, de la désactivation, de la révocation ou du retrait de tous les droits d’accès). |
|  | Vérifier que l’entité responsable a :   1. déclenché le retrait d’accès physique sans accompagnement et d’accès *distant interactif* d’une personne lors de son départ; et 2. mené à bien ce processus dans un délais de 24 heures suivant le départ (le retrait d’accès peut différer de la suppression, de la désactivation, de la révocation ou du retrait de tous les droits d’accès). |
| **Notes pour l’auditeur:**  Le retrait de la capacité d’accès ne requiert pas la suppression ou la désactivation des comptes utilisateurs de la personne. La capacité d’accès d’un individu peut être retirée en désactivant l’accès de la personne au réseau, en confisquant son badge, ou par tout autre moyen approprié. Le retrait d’*accès distant interactif* peut être accompli, par exemple, en désactivant l’authentification multi-facteurs de l’individu. | |

**Notes des auditeurs:**

**E5 Alinéa 5.2**

| **Tableau E5 (CIP-004-6) – Révocation d’accèes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.2 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Dans le cas d’une réaffectation ou d’une mutation, révoquer l’accès électronique autorisé aux comptes individuels et l’accès physique sans accompagnement autorisé que l’entité responsable juge non nécessaires avant la fin du jour civil suivant la date, déterminée par l’entité responsable, où la personne n’a plus besoin de ces accès. | Exemples non limitatifs de pièces justificatives :   1. formulaire d’activité ou d’approbation daté attestant l’examen des accès logique et physique ; et 2. journaux ou autres pièces justificatives attestant que la personne ne dispose plus des accès que l’entité responsable détermine comme n’étant plus nécessaires. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E4, alinéa 5.2**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes de révocation d’accès électronique autorisé aux comptes individuels et d’accès physique sans accompagnement autorisés d’un individu lors d’une réaffectation ou d’une mutation. Cette révocation devrait être appliquée avant la fin du jour civil suivant la date déterminée par l’entité responsable où la personne n’a plus besoin de ces accès. |
|  | Dans le cas d’une réaffectation ou d’une mutation, vérifier que l’entité responsable a révoqué l’accès électronique autorisé aux comptes individuels et l’accès physique sans accompagnement autorisés d’un individu, avant la fin du jour civil suivant la date déterminée par l’entité responsable où la personne n’a plus besoin de ces accès. |
| **Notes pour l’auditeur:**  La révocation d’accès ne nécessite pas obligatoirement la suppression des comptes de l’individu. Le compte peut être désactivé au lieu d’être supprimé. | |

**Notes des auditeurs:**

**E5 Alinéa 5.3**

| **Tableau E5 (CIP-004-6) – Révocation d’accèes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.3 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les PACS associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; et 2. les *PACS* associés. | Dans le cas d’un départ, révoquer l’accès de la personne aux emplacements de stockage désignés pour l’information de *système électronique BES*, qu’ils soient physiques ou électroniques (à moins que l’accès ait déjà été révoqué selon l’exigence E5.1), avant la fin du jour civil suivant la date à laquelle prend effet le départ. | Exemple non limitatif de pièce justificative : formulaire d’activité ou d’approbation attestant le retrait de l’accès aux emplacements physiques ou aux systèmes électroniques désignés pour l’information de *système électronique BES* daté au plus tard du jour civil suivant le départ. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E4, alinéa 5.3**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes de révocation d’accès suivant un départ, afin de révoquer l’accès d’un individu aux emplacements de stockage désignés pour l’information de *système électronique BES*, qu’ils soient physiques ou électroniques (à moins que l’accès ait déjà été révoqué selon l’exigence E5.1), avant la fin du jour civil suivant la date à laquelle prend effet le départ. |
|  | À la suite d’un départ, vérifier que l’entité responsable a révoqué l’accès de l’individu aux emplacements de stockage désignés pour l’information de *système électronique BES*, qu’ils soient physiques ou électroniques (à moins que l’accès ait déjà été révoqué selon l’exigence E5.1), avant la fin du jour civil suivant la date à laquelle prend effet le départ. |
| **Notes pour l’auditeur:**   1. Si l’accès avait déjà été retiré selon l’exigence E5.1, aucune autre mesure n’est requise. 2. La révocation des accès ne requiert pas la suppression ou la désactivation des comptes de l’individu. La capacité d’accès d’un individu peut être retirée en désactivant l’accès de la personne au réseau, en confisquant son badge, ou par tout autre moyen approprié. 3. Le retrait d’*accès distant interactif* peut être accompli, par exemple, en désactivant l’authentification multi-facteurs de l’individu. | |

**Notes des auditeurs:**

**E5 Alinéa 5.4**

| **Tableau E5 (CIP-004-6) – Révocation d’accèes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.4 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés. | Dans le cas d’un départ, révoquer l’accès aux comptes utilisateurs non partagés de la personne (à moins que l’accès ait déjà été révoqué selon l’exigence E5.1 ou E5.3) dans les 30 jours civils suivant la date à laquelle prend effet le départ. | Exemple non limitatif de pièce justificative : formulaire d’activité ou d’approbation attestant le retrait de l’accès à un *actif électronique BES* ou à un logiciel d’application selon ce qui est jugé nécessaire pour mener à bien la révocation d’accès, et daté dans les 30 jours civils suivant le départ. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E4, alinéa 5.4**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes de révocation d’accès à la suite d’un départ, visant à révoquer l’accès aux comptes utilisateurs non partagés de la personne (à moins que l’accès ait déjà été révoqué selon l’exigence E5.1 ou E5.3) dans les 30 jours civils suivant la date à laquelle prend effet le départ. |
|  | À la suite du départ d’un individu, vérifier que l’entité responsable a révoqué l’accès aux comptes utilisateurs non partagés de la personne (à moins que l’accès ait déjà été révoqué selon l’exigence E5.1 ou E5.3) dans les 30 jours civils suivant la date à laquelle le départ prend effet. |
| **Notes pour l’auditeur:**  La révocation d’accès ne nécessite pas obligatoirement la suppression des comptes de l’individu. Le compte peut être désactivé eu lieu d’être supprimé. | |

**Notes des auditeurs:**

**E5 Alinéa 5.5**

| **Tableau E5 (CIP-004-6) – Révocation d’accèes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.5 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés. | Dans le cas d’un départ, changer les mots de passe des comptes partagés connus de l’utilisateur dans les 30 jours civils suivant le départ. Dans le cas d’une réaffectation ou d’une mutation, changer les mots de passe des comptes partagés connus de l’utilisateur dans les 30 jours civils suivant la date, déterminée par l’entité responsable, où la personne n’a plus besoin de cet accès.  Si l’entité responsable détermine et documente qu’un délai plus long est nécessaire en raison de circonstances opérationnelles atténuantes, changer les mots de passe dans les 10 jours civils suivant la fin de ces circonstances. | Exemples non limitatifs de pièces justificatives :   1. formulaire d’activité ou d’approbation attestant que le mot de passe a été changé dans les 30 jours civils suivant le départ ; 2. formulaire d’activité ou d’approbation attestant que le mot de passe a été changé dans les 30 jours civils suivant la réaffectation ou la mutation ; ou 3. documentation des circonstances opérationnelles atténuantes et formulaire d’activité ou d’approbation attestant que le mot de passe a été changé dans les 10 jours civils suivant la fin de ces circonstances. |

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

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

**Démarche d’évaluation de la conformité spécifique à la norme CIP-004-6, E4, alinéa 5.5**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs programmes de révocation d’accès suivant un départ, afin de changer les mots de passe du ou des comptes partagés connus de l’utilisateur dans les 30 jours civils suivant son départ. Dans le cas d’une réaffectation ou d’une mutation, afin de changer les mots de passe du ou des comptes partagés connus de l’utilisateur dans les 30 jours civils suivant la date, déterminée par l’entité responsable, où la personne n’a plus besoin de ces accès.  Le ou les processus peuvent comprendre des dispositions permettant à l’entité responsable de déterminer et documenter qu’un délai plus long est nécessaire en raison de circonstances opérationnelles atténuantes, auquel cas le ou les mots de passe peuvent être changés dans les 10 jours civils suivant la fin de ces circonstances. |
|  | Si des circonstances opérationnelles atténuantes sont invoquées, vérifier que les circonstances ont été documentées et comportent une date de fin spécifique. |
|  | Dans le cas d’un départ où l’entité responsable n’invoque pas de circonstances opérationnelles atténuantes, vérifier que les mots de passe des comptes partagés connus de l’utilisateur ont été changés dans les 30 jours civils suivant son départ. |
|  | Dans le cas d’un départ où l’entité responsable invoque des circonstances opérationnelles atténuantes, vérifier que les mots de passe des comptes partagés connus de l’utilisateur ont été changés dans les 10 jours civils suivant la date de fin des circonstances opérationnelles atténuantes. |
|  | Dans le cas d’une réaffectation ou d’une mutation où l’entité responsable n’invoque pas de circonstances opérationnelles atténuantes, vérifier que les mots de passe des comptes partagés connus de l’utilisateur ont été changés dans les 30 jours civils suivant la date, déterminée par l’entité responsable, où la personne n’a plus besoin de ces accès. |
|  | Dans le cas d’une réaffectation ou d’une mutation où l’entité responsable invoque des circonstances opérationnelles atténuantes, vérifier que les mots de passe des comptes partagés connus de l’utilisateur ont été changés dans les 10 jours civils suivant la date de fin des circonstances opérationnelles atténuantes. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**Information supplémentaire**

**Norme de fiabilité**

Le texte complet de la norme CIP-004-6 peut être consulté sur le site internet de la Régie de l’énergie, à la section [surveillance de la conformité](http://www.regie-energie.qc.ca/audiences/NormesFiabiliteTransportElectricite/index.html).



**Historique des révisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Réviseurs** | **Description de la révision** |
| 1 | Juin 2018 | Document initial | Document créé à partir du formulaire « RSAW » de la NERC |
| 2 | Février 2022 | Régie de l’énergie | Changement de gabarit |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Date(s) d’évaluation de la conformité: la ou les dates auxquelles l’évaluation de la conformité réelle (audit sur place, audit hors site, contrôle ponctuel, etc.) a lieu. [↑](#footnote-ref-1)