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

# CIP-007-6 — Cybersécurité – Gestion de la sécurité des systèmes

***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 |  |  |  |
| A1.2 |  |  |  |
| **E2** |  |  |  |
| A2.1 |  |  |  |
| A2.2 |  |  |  |
| A2.3 |  |  |  |
| A2.4 |  |  |  |
| **E3** |  |  |  |
| A3.1 |  |  |  |
| A3.2 |  |  |  |
| A3.3 |  |  |  |
| **E4** |  |  |  |
| A4.1 |  |  |  |
| A4.2 |  |  |  |
| A4.3 |  |  |  |
| A4.4 |  |  |  |
| **E5** |  |  |  |
| A5.1 |  |  |  |
| A5.2 |  |  |  |
| A5.3 |  |  |  |
| A5.4 |  |  |  |
| A5.5 |  |  |  |
| A5.6 |  |  |  |
| A5.7 |  |  |  |

|  |  |
| --- | --- |
| **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-007-6) – Ports et services. *[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation le même jour]*
2. Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-007-6) – Ports et services ; d’autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

**E1 Alinéa 1.1**

| **Tableau E1 (CIP-007-6) – Ports et services** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.1 | *Systèmes électroniques BES* à impact élevé et :   1. les EACMS associés ; 2. les PACS associés ; et 3. les PCA associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les EACMS associés ; 2. les PACS associés ; et 3. les PCA associés. | Si cela est techniquement faisable, activer uniquement les ports logiques accessibles par le réseau qui sont jugés nécessaires par l’entité responsable, y compris les plages de ports ou de services qui sont nécessaires pour la prise en charge de ports dynamiques.  Si un dispositif ne permet pas la désactivation ou la restriction de ses ports logiques, tous les ports ouverts sont considérés comme nécessaires. | Exemples non limitatifs de pièces justificatives :   * documentation établissant la nécessité de tous les ports activés de tous les *actifs électroniques* et *points d’accès électronique* visés, pris individuellement ou collectivement ; * listes des ports d’écoute des *actifs électroniques*, pris individuellement ou collectivement, provenant des fichiers de configuration des dispositifs, du résultat de commandes comme netstat ou de balayages réseau des ports ouverts ; ou * fichiers de configuration des pare-feu (de type hôte) ou de tout autre mécanisme intégré au matériel qui n’autorisent l’accès qu’aux ports nécessaires et qui le refusent à tous les autres. |

**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-007-6, E1, alinéa 1.1**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour activer uniquement les ports logiques accessibles par le réseau qui sont jugés nécessaires par l’entité responsable, y compris les plages de ports ou de services qui sont nécessaires pour la prise en charge de ports dynamiques, si cela est techniquement faisable. Si un dispositif ne permet pas la désactivation ou la restriction de ses ports logiques, tous les ports ouverts sont considérés comme nécessaires. |
|  | Si l’entité déclare qu’un *actif électronique* d’un système visé qui ne permet pas la désactivation ou la restriction de ses ports logiques, vérifier l’authenticité de cette affirmation.  Vérifier chacun des cas où l’*actif électronique* d’un système visé ne permet pas la désactivation ou la restriction des ports logiques. |
|  | Pour chaque *actif électronique* d’un système visé qui permet la désactivation ou la restriction des ports logiques, pour chaque plage de ports logiques ou de service activés nécessaires à la prise en charge de ports dynamiques, vérifier un des éléments suivants :   * La documentation établissant la nécessité de la plage de ports ou de service ; ou * L’exception pour raison technique (« TFE ») accordée pour la plage de ports ou de services. |
|  | Pour chaque *actif électronique* d’un système visé qui permet la désactivation ou la restriction des ports logiques, pour chaque port logique accessibles par le réseau de l’*actif électronique*, vérifier un des éléments suivants :   * La documentation établissant la nécessité du port logique accessible par le réseau; ou * La « TFE » accordée pour le port logique accessible par le réseau. |
|  | Si une « TFE » s’applique à cet alinéa, vérifier que les mesures compensatoires identifiées à la « TFE » ont été mises en œuvre. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E1 Alinéa 1.2**

| **Tableau E1 (CIP-007-6) – Ports et services** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.2 | *Systèmes électroniques BES* à impact élevé et :   1. les *PCA* associés ; et 2. les composants de communication non programmables associés situés à la fois dans un *périmètre de sécurité physique* et dans un *périmètre de sécurité électronique*.   *Systèmes électroniques BES* à impact moyen de *centres de contrôle* et :   1. les *PCA* associés ; et 2. les composants de communication non programmables associés situés à la fois dans un *périmètre de sécurité physique* et dans un *périmètre de sécurité électronique*. | Empêcher l’utilisation de ports d’entrée-sortie physiques non nécessaires utilisés pour la connectivité de réseau, les commandes pupitre ou les *supports de stockage amovibles*. | Exemple non limitatif de pièces justificatives : documentation indiquant le type de protection assurée pour les ports d’entrée-sortie physiques – soit logique (configuration du système), soit physique (verrouillage ou signalisation). |

**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-007-6, E1, alinéa 1.2**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour empêcher l’utilisation de ports d’entrée-sortie physiques non nécessaires utilisés pour la connectivité de réseau, les commandes pupitre ou les *supports de stockage amovibles*. |
|  | Pour chaque *actif électronique* d’un système visé, vérifier que l’entité responsable a empêché l’utilisation des ports d’entrée-sortie physiques non nécessaires utilisés pour la connectivité de réseau, les commandes pupitre ou les *supports de stockage amovibles*. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E2 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 E2 (CIP-007-6) – Gestion des correctifs de sécurité. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l’exploitation]*
2. Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité ; d’autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

**E2 Alinéa 2.1**

| **Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.1 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés; et 3. les *PCA* associés. | Un processus de gestion des correctifs portant sur le suivi, l’évaluation et l’installation des correctifs de cybersécurité pour les *actifs électroniques* visés. Le suivi comprend la désignation de la ou des sources que l’entité responsable utilise pour faire le suivi de la publication de correctifs de cybersécurité destinés aux *actifs électroniques* visés qui sont actualisables et pour lesquels il existe une source de correctifs. | Exemples non limitatifs de pièces justificatives : documentation d’un processus de gestion des correctifs et documentation ou listes de sources qui sont utilisées pour le suivi visant chacun des *systèmes électroniques BES* ou des *actifs électroniques 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-007-6, E2, alinéa 2.1**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus de gestion des correctifs portant sur le suivi, l’évaluation et l’installation des correctifs de cybersécurité pour les *actifs électroniques* visés. |
|  | Vérifier que la partie suivi de chaque processus de gestion des correctif comprend la désignation de la ou des sources que l’entité responsable utilise pour faire le suivi de la publication de correctifs de cybersécurité destinés aux *actifs électroniques* visés qui sont actualisables et pour lesquels il existe une source de correctifs. |
|  | Pour chaque *actif électronique* visé, vérifier qu’au moins un des éléments suivants est vrai :   * L’entité responsable a identifié une ou plusieurs sources de correctifs ; * L’entité responsable a documenté que l’*actif électronique* ne peut être mis à jour ; ou * L’entité responsable a documenté qu’aucune source de correctifs n’existe. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E2 Alinéa 2.2**

| **Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.2 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Au moins une fois tous les 35 jours civils, évaluer l’applicabilité des correctifs de sécurité publiés par la ou les sources indiquées à l’alinéa 2.1 depuis l’évaluation précédente. | Exemple non limitatif de pièces justificatives : une évaluation effectuée ou citée par une entité responsable ou réalisée en son nom et portant sur les correctifs de sécurité publiés par les sources documentées, et ce, au moins tous les 35 jours civils. |

**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-007-6, E2, alinéa 2.2**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour évaluer l’applicabilité des correctifs de sécurité publiés par la ou les sources indiquées à l’alinéa 2.1 depuis l’évaluation précédente, au moins une fois tous les 35 jours civils. |
|  | Pour chaque source de correctifs indiquée, vérifier que l’applicabilité des correctifs de sécurité a été évaluée au moins une fois tous les 35 jours civils. |
|  | Pour chaque source de correctifs indiquée, vérifier les résultats des évaluations portant sur l’applicabilité. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E2 Alinéa 2.3**

| **Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.3 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Pour les correctifs jugés applicables selon l’alinéa 2.2, prendre une des mesures suivantes dans les 35 jours civils suivant la fin de l’évaluation :   * appliquer les correctifs applicables ; * créer un plan d’atténuation daté ; ou * réviser un plan d’atténuation existant.   Les plans d’atténuation doivent comprendre les mesures que l’entité responsable compte prendre pour atténuer les vulnérabilités visées par chaque correctif de sécurité, ainsi qu’un délai de mise en œuvre de ces mesures. | Exemples non limitatifs de pièces justificatives :   * enregistrements d’installation des correctifs (p. ex. rapport exporté d’un outil automatisé de gestion des correctifs indiquant la date d’installation, validation de la version du logiciel des composants du *système électronique BES* ou exportation d’un registre indiquant que le logiciel a été installé) ; ou * plan daté indiquant à quel moment et de quelle façon la vulnérabilité sera corrigée, qui documente les mesures que l’entité responsable compte prendre pour atténuer les vulnérabilités visées par le correctif de sécurité et qui précise un délai d’exécution des mesures d’atténuation. |

**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-007-6, E2, alinéa 2.3**

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

|  |  |
| --- | --- |
|  | Pour les correctifs jugés applicables selon l’alinéa 2.2, vérifier que l’entité responsable a documenté un ou plusieurs processus afin de prendre une des mesures suivantes dans les 35 jours civils suivants la fin de l’évaluation :   * appliquer les correctifs applicables ; * créer un plan d’atténuation daté ; ou * réviser un plan d’atténuation existant. |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour ses plans d’atténuation qui exigent l’inclusion des mesures que l’entité responsable compte prendre pour atténuer les vulnérabilités visées par chaque correctif de sécurité, ainsi qu’un délai de mise en œuvre de ces mesures. |
|  | Pour chaque correctif de sécurité applicable, vérifier que l’une des mesures suivantes a été prise dans les 35 jours civils suivants la fin de l’évaluation portant sur l’applicabilité :   * Le correctif a été appliqué à tous les dispositifs auxquels il s’applique ; * Un plan d’atténuation a été créé ; ou * Un plan d’atténuation a été révisé. |
|  | Si un plan d’atténuation a été créé ou révisé, vérifier que le plan d’atténuation comprend des mesures prévues pour atténuer les vulnérabilités visées par chaque correctif de sécurité, ainsi qu’un délai de mise en œuvre de ces mesures. |
| **Notes pour l’auditeur:**  Les entités peuvent choisir d’utiliser un seul plan d’atténuation pour plusieurs correctifs, auquel cas le plan d’atténuation doit comprendre des mesures prévues pour atténuer les vulnérabilités visées par chaque correctif de sécurité. | |

**Notes des auditeurs:**

**E2 Alinéa 2.4**

| **Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.4 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Pour chaque plan d’atténuation créé ou mis à jour selon l’alinéa 2.3, mettre le plan en œuvre dans le délai qui y est précisé, à moins qu’une révision du plan ou un prolongement du délai indiqué à l’alinéa 2.3 soit approuvé par le *cadre supérieur CIP* ou son délégataire. | Exemple non limitatif de pièces justificatives : registres de mise en œuvre des plans d’atténuation. |

**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-007-6, E2, alinéa 2.4**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus qui exigent, pour chaque plan d’atténuation créé ou mis à jour selon l’alinéa 2.3, la mise en œuvre du plan d’atténuation dans le délais qui y est précisé, à moins qu’une révision du plan ou un prolongement du délai indiqué à l’alinéa 2.3 soit approuvé par le *cadre supérieur CIP* ou son délégataire. |
|  | Pour chaque plan d’atténuation complété :   1. Vérifier que le plan d’atténuation a été complété par la mise en œuvre de toutes les mesures du plan d’atténuation ; 2. Vérifier que le plan d’atténuation a été complété dans le délais qui y est spécifié ; et 3. Si une révision ou un prolongement a été apporté à un plan d’atténuation, vérifier que la révision ou le prolongement a été approuvé par le *cadre supérieur CIP* ou son délégataire. |
|  | Pour chaque plan d’atténuation en vigueur :   1. Vérifier que le délai de mise en œuvre du plan d’atténuation n’a pas été dépassé, ou son prolongement approuvé, le cas échéant. 2. Si une révision ou un prolongement a été apporté à un plan d’atténuation, vérifier que la révision ou le prolongement a été approuvé par le *cadre supérieur CIP* ou son délégataire. |
| **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 processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-007-6) – Protection contre les programmes malveillants. *[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation le même jour]*
2. Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E3(CIP-007-6) – Protection contre les programmes malveillants ; d’autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

**E3 Alinéa 3.1**

| **Tableau E3 (CIP-007-6) – Protection contre les programmes malveillants** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.1 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Utiliser une ou des méthodes pour bloquer, détecter ou prévenir les programmes malveillants. | Exemple non limitatif de pièces justificatives : suivis de la mise en œuvre de ces méthodes par l’entité responsable (au moyen de logiciels antivirus habituels, du renforcement des systèmes, de politiques, 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-007-6, E3, alinéa 3.1**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus visant à utiliser une ou des méthodes pour bloquer, détecter ou prévenir les programmes malveillants. |
|  | Vérifier que chaque système visé a une ou plusieurs méthodes documentées pour bloquer, détecter ou prévenir les programmes malveillants. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E3 Alinéa 3.2**

| **Tableau E3 (CIP-007-6) – Protection contre les programmes malveillants** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.2 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Atténuer la menace des programmes malveillants détectés. | Exemples non limitatifs de pièces justificatives :   * registres des processus d’intervention en cas de détection de programmes malveillants ; * suivis de la performance de ces processus lorsque des programmes malveillants sont détectés. |

**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-007-6, E3, alinéa 3.2**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus visant à atténuer la menace des programmes malveillants détectés. |
| **Notes pour l’auditeur:**  Chaque programme malveillant n’a pas forcément besoin d’être supprimé d’un dispositif afin d’atténuer la menace de ce programme malveillant. Par exemple, il peut être possible de confiner un programme malveillant en empêchant la communication avec le serveur de contrôle et de commande et en prévenant sa propagation à d’autres systèmes. Le programme malveillant peut ensuite être supprimé ultérieurement, par exemple pendant un retrait planifié. | |

**Notes des auditeurs:**

**E3 Alinéa 3.3**

| **Tableau E3 (CIP-007-6) – Protection contre les programmes malveillants** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.3 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Pour les méthodes indiquées à l’alinéa 3.1 qui utilisent des signatures ou des séquences de code, avoir un processus de mise à jour des signatures et des séquences de code. Le processus doit traiter de l’essai et de l’installation des signatures et des séquences de code. | Exemple non limitatif de pièces justificatives : documentation décrivant le processus de mise à jour des signatures et des séquences de code. |

**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-007-6, E3, alinéa 3.3**

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

|  |  |
| --- | --- |
|  | Pour les méthodes indiquées à l’alinéa 3.1 qui utilisent des signatures ou des séquences de code, vérifier que l’entité responsable a documenté un ou plusieurs processus de mise à jour des signatures et des séquences de code. Le processus doit traiter de l’essai et de l’installation des signatures et des séquences de code. |
|  | Pour chaque méthode utilisée pour bloquer, détecter ou prévenir les programmes malveillants qui utilisent des signatures ou des séquences de code, vérifier que le processus associé traite de l’essai et de l’installation des mises à jour aux signatures et aux séquences de code. |
|  | Pour chaque méthode utilisée pour bloquer, détecter ou prévenir les programmes malveillants qui utilisent des signatures ou des séquences de code, vérifier que le processus associé a été mis en œuvre. |
| **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 processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-007-6) – Surveillance des événements de sécurité. *[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation le même jour et évaluation des activités d’exploitation]*
2. Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-007-6) – Surveillance des événements de sécurité ; d’autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

**E4 Alinéa 4.1**

| **Tableau E4 (CIP-007-6) – Surveillance des événements de sécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.1 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Journaliser les événements au niveau du *système électronique BES* (selon les capacités du *système électronique BES*) ou au niveau de l’*actif électronique* (selon les capacités de l’*actif électronique*) permettant la détection des *incidents de cybersécurité* – et les enquêtes subséquentes à leur sujet – qui comprennent au minimum chacun des types d’événements suivants :   * + 1. toute tentative détectée d’ouverture de session ayant réussi ;     2. toute tentative détectée d’accès ou d’ouverture de session ayant échoué ; et     3. tout programme malveillant détecté. | Exemples non limitatifs de pièces justificatives : liste des types d’événements que le *système électronique BES* est en mesure de détecter, générée manuellement ou automatiquement, et, le cas échéant, qu’il est configuré pour journaliser. Cette liste doit comprendre les types d’événements obligatoires. |

**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-007-6, E4, alinéa 4.1**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour journaliser les événements au niveau du *système électronique BES* (selon les capacités du *système électronique BES*) ou au niveau de l’*actif électronique* (selon les capacités de l’*actif électronique*) permettant la détection des *incidents de cybersécurité* – et les enquêtes subséquentes à leur sujet – qui comprennent au minimum chacun des types d’événements suivants :   1. Toute tentative détectée d’ouverture de session ayant réussi ; 2. Toute tentative détectée d’accès ou d’ouverture de session ayant échoué ; et 3. Tout programme malveillant détecté. |
|  | Pour chaque type d’évènements permettant la détection ou les enquêtes subséquentes des *incidents de cybersécurité*:   * Si la journalisation de l’évènement est effectuée au niveau du *système électronique BES*, pour chaque système visé, vérifier que :   + le *système électronique BES* est capable de, et configuré pour, journaliser le type d’évènement;   + le *système électronique BES* génère des journaux du type d’évènement; ou   + le *système électronique BES* n’est pas capable de journaliser le type d’évènement. * Si la journalisation de l’évènement est effectuée au niveau de l’*actif électronique*, pour chaque *actif électronique* d’un système visé, vérifier que :   + l’*actif électronique* est capable de, et configuré pour, journaliser le type d’évènement;   + l’*actif électronique* génère des journaux du type d’évènement; ou   + l’*actif électronique* n’est pas capable de journaliser le type d’évènement. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E4 Alinéa 4.2**

| **Tableau E4 (CIP-007-6) – Surveillance des événements de sécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.2 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Générer des alertes pour les événements de sécurité qui, selon l’entité responsable, nécessitent une alerte, y compris au minimum chacun des types d’événements suivants (selon les capacités de l’*actif électronique* ou du *système électronique BES*) :   * + 1. programmes malveillants détectés conformément à l’alinéa 4.1 ; et     2. échec détecté de la journalisation des événements définis à l’alinéa 4.1. | Exemples non limitatifs de pièces justificatives : liste, générée manuellement ou automatiquement, des événements de sécurité qui, selon l’entité responsable, nécessitent des alertes, y compris une liste, générée manuellement ou automatiquement, indiquant la configuration des alertes. |

**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-007-6, E4, alinéa 4.2**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour générer des alertes pour les événements de sécurité qui, selon l’entité responsable, nécessitent une alerte, y compris au minimum chacun des types d’événements suivants (selon les capacités de l’*actif électronique* ou du *système électronique BES*) :   1. programmes malveillants détectés conformément à l’alinéa 4.1 ; et 2. échec détecté de la journalisation des événements définis à l’alinéa 4.1. |
|  | Vérifier que l’entité responsable a déterminé les évènements de sécurité qui nécessitent une alerte. |
|  | Vérifier que les évènements de sécurité qui nécessitent une alerte comprennent, au minimum :   1. programmes malveillants détectés; et 2. échec détecté de la journalisation des événements définis à l’alinéa 4.1. |
|  | Pour chaque évènement de sécurité qui nécessite une alerte :   1. Si l’alerte est générée selon les capacités de l’*actif électronique*, est-ce que l’*actif électronique* a la capacité de générer des alertes pour ce type d’évènement ? 2. Si oui, vérifier l’un ou l’autre : 3. L’alerte est configurée selon l’*actif électronique* pour le type d’évènement de sécurité ; ou 4. Une alerte réelle a été générée. 5. Sinon, vérifier l’incapacité de l’*actif électronique* de générer une alerte pour ce type d’évènement. 6. Si l’alerte est générée selon les capacités du *système électronique BES*, est-ce que le *système électronique BES* a la capacité de générer des alertes pour ce type d’évènement ? 7. Si oui, vérifier l’un ou l’autre : 8. L’alerte est configurée selon le *système électronique BES* pour le type d’évènement de sécurité ; ou 9. Une alerte réelle a été générée. 10. Sinon, vérifier l’incapacité du *système électronique BES* de générer une alerte pour ce type d’évènement. |
| **Notes pour l’auditeur :** | |

**Notes des auditeurs:**

**E4 Alinéa 4.3**

| **Tableau E4 (CIP-007-6) – Surveillance des événements de sécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.3 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen de *centres de contrôle* et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Si cela est techniquement faisable, conserver les journaux des événements exigés à l’alinéa 4.1 pendant au moins 90 jours civils consécutifs, sauf dans des *circonstances CIP exceptionnelles*. | Exemples non limitatifs de pièces justificatives : documentation du processus de conservation des journaux des événements et rapports générés manuellement ou automatiquement qui indiquent que la configuration de conservation des journaux est réglée à 90 jours ou plus. |

**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-007-6, E4, alinéa 4.3**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour conserver les journaux des événements exigés à l’alinéa 4.1 pendant au moins 90 jours civils consécutifs, sauf dans des *circonstances CIP exceptionnelles*. |
|  | Pour chaque système visé, vérifier que les journaux sont conservés pendant au moins 90 jours civils consécutifs, sauf si :   * Une « TFE » a été accordée pour le système visé ; ou * Une *circonstance CIP exceptionnelle* documentée existe. |
|  | Si une « TFE » s’applique à cet alinéa, vérifier que les mesures compensatoires identifiées à la « TFE » ont été mises en œuvre. |
|  | Si l’entité responsable a répondu à des *circonstances CIP exceptionnelles*, vérifiez que l’entité responsable a respecté les politiques de cybersécurité applicables. |
| **Notes pour l’auditeur:**  L'entité responsable peut faire référence à un ensemble distinct de documents afin de démontrer sa conformité à toutes les exigences touchées par des *circonstances CIP exceptionnelles*. | |

**Notes des auditeurs:**

**E4 Alinéa 4.4**

| **Tableau E4 (CIP-007-6) – Surveillance des événements de sécurité** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.4 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; et 2. les *PCA* associés. | Examiner un résumé ou un échantillon des événements journalisés, tels que définis par l’entité responsable, à intervalles d’au plus 15 jours civils, afin de repérer les *incidents de cybersécurité* non détectés. | Exemples non limitatifs de pièces justificatives : document décrivant l’examen et ses constatations éventuelles, et document daté démontrant que l’examen a eu lieu. |

**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-007-6, E4, alinéa 4.4**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus visant à examiner un résumé ou un échantillon des événements journalisés, tels que définis par l’entité responsable, à intervalles d’au plus 15 jours civils, afin de repérer les *incidents de cybersécurité* non détectés. |
|  | Vérifier que l’entité responsable examine un résumé ou un échantillon des évènements journalisés au moins une fois tous les 15 jours civils afin de repérer les *incidents de cybersécurité* non détectés. |
| **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 processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l’exploitation]*
2. Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes ; d’autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

**E5 Alinéa 5.1**

| **Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.1 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen de *centres de contrôle* et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Avoir une ou plusieurs méthodes pour imposer l’authentification de tout accès utilisateur interactif, si cela est techniquement faisable. | Exemple non limitatif de pièces justificatives : documentation décrivant le mode d’authentification des 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-007-6, E4, alinéa 5.1**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour avoir une ou plusieurs méthodes pour imposer l’authentification de tout accès utilisateur interactif, si cela est techniquement faisable. |
|  | Pour chaque système visé, vérifier l’un ou l’autre :   * L’entité responsable impose l’authentification de tout accès utilisateur interactif ; ou * Une « TFE » a été accordée pour cette circonstance. |
|  | Si une « TFE » s’applique à cet alinéa, vérifier que les mesures compensatoires identifiées à la « TFE » ont été mises en œuvre. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E5 Alinéa 5.2**

| **Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.2 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Répertorier par système, par groupe de systèmes, par emplacement ou par type de système tous les comptes par défaut ou autres comptes génériques qui sont connus et activés. | Exemple non limitatif de pièces justificatives : liste de comptes indiquant les types de comptes activés ou génériques utilisés pour le *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-007-6, E4, alinéa 5.2**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour répertorier par système, par groupe de systèmes, par emplacement ou par type de système tous les comptes par défaut ou autres comptes génériques qui sont connus et activés. |
|  | Pour chaque *actif électronique* d’un système visé, vérifier que l’entité responsable a répertorié tous les comptes par défaut ou autres comptes génériques qui sont connus et activés. Ces types de comptes peuvent être répertoriés par système, par groupe de systèmes, par emplacement ou par type de système. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E5 Alinéa 5.3**

| **Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.3 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Recenser toutes les personnes ayant un accès autorisé à des comptes partagés. | Exemple non limitatif de pièces justificatives : liste des comptes partagés et des personnes qui y ont un accès autorisé. |

**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-007-6, E4, alinéa 5.3**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour recenser toutes les personnes ayant un accès autorisé à des comptes partagés. |
|  | Pour chaque *actif électronique* d’un système visé, vérifier que l’entité responsable a recensé toutes les personnes ayant un accès autorisé à des comptes partagés. |
| **Notes pour l’auditeur:**  L'entité responsable a une marge de manœuvre dans la façon dont les comptes partagés peuvent être documentés. Les comptes partagés peuvent être documentés par *actif électronique* ou par *système électronique BES*. De plus, les personnes ayant un accès autorisé à des comptes partagés peuvent être énumérées individuellement ou par rôle. | |

**Notes des auditeurs:**

**E5 Alinéa 5.4**

| **Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.4 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Changer les mots de passe par défaut connus, selon les capacités de l’*actif électronique*. | Exemples non limitatifs de pièces justificatives :   * documentation de l’exécution d’une procédure selon laquelle les mots de passe sont changés lorsque de nouveaux dispositifs sont en service ; ou * mention dans les manuels des systèmes ou dans d’autres documents de leurs fournisseurs selon laquelle les mots de passe par défaut ont été générés de façon pseudo-aléatoire et sont donc exclusifs à chaque dispositif. |

**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-007-6, E4, alinéa 5.4**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour changer les mots de passe par défaut connus, selon les capacités de l’*actif électronique*. |
|  | Pour les *actif électroniques* des systèmes visés ayant la capacité de changer les mots de passe par défaut, vérifier que l’entité responsable a changé les mots de passe par défaut connus. |
|  | Pour les *actif électroniques* des systèmes visés n’ayant pas la capacité de changer les mots de passe par défaut, vérifier cette incapacité. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E5 Alinéa 5.5**

| **Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.5 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | En ce qui concerne l’authentification uniquement par mot de passe de l’accès utilisateur interactif, imposer les paramètres suivants par des moyens techniques ou procéduraux :   * + 1. une longueur de mot de passe d’au moins huit caractères ou de la longueur maximale permise par l’*actif électronique*, selon la moindre des deux ; et     2. une complexité minimale du mot de passe d’au moins trois types différents de caractères (lettres majuscules, lettres minuscules, chiffres, caractères non alphanumériques, etc.) ou du maximum permis par l’*actif électronique*, selon la moindre des deux. | Exemples non limitatifs de pièces justificatives :   * rapports générés automatiquement ou captures d’écran montrant les paramètres de mot de passe appliqués par le système, y compris la longueur et la complexité ; ou * attestations comportant un renvoi aux procédures documentées ayant été suivies. |

**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-007-6, E4, alinéa 5.5**

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

|  |  |
| --- | --- |
|  | Pour l’authentification uniquement par mot de passe de l’accès utilisateur interactif, vérifier que l’entité responsable a documenté un ou plusieurs processus pour imposer les paramètres suivants par des moyens techniques ou procéduraux :   1. une longueur de mot de passe d’au moins huit caractères ou de la longueur maximale permise par l’*actif électronique*, selon la moindre des deux ; et 2. une complexité minimale du mot de passe d’au moins trois types différents de caractères (lettres majuscules, lettres minuscules, chiffres, caractères non alphanumériques, etc.) ou du maximum permis par l’*actif électronique*, selon la moindre des deux. |
|  | Pour l’authentification uniquement par mot de passe de l’accès utilisateur interactif de chaque *actif électronique* des systèmes visés, vérifier que la longueur de mot de passe est imposée par des moyens techniques ou procéduraux, selon l’alinéa 5.5.1. |
|  | Pour l’authentification uniquement par mot de passe de l’accès utilisateur interactif de chaque *actif électronique* des systèmes visés, vérifier que la complexité du mot de passe est imposée par des moyens techniques ou procéduraux, selon l’alinéa 5.5.2. |
| **Notes pour l’auditeur:**  Cet alinéa ne s’applique pas à l’authentification multifactorielle. | |

**Notes des auditeurs:**

**E5 Alinéa 5.6**

| **Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.6 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Si cela est techniquement faisable, pour toute authentification uniquement par mot de passe de l’accès utilisateur interactif, imposer par des moyens techniques ou procéduraux les changements de mot de passe ou l’obligation de changer le mot de passe au moins une fois tous les 15 mois civils. | Exemples non limitatifs de pièces justificatives :   * rapports générés automatiquement ou captures d’écran montrant la fréquence de changement de mot de passe appliquée par le système ; ou * attestations comportant un renvoi aux procédures documentées ayant été suivies. |

**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-007-6, E4, alinéa 5.6**

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

|  |  |
| --- | --- |
|  | Pour toute authentification uniquement par mot de passe de l’accès utilisateur interactif, vérifier que l’entité responsable a documenté un ou plusieurs processus pour imposer par des moyens techniques ou procéduraux les changements de mot de passe ou l’obligation de changer le mot de passe au moins une fois tous les 15 mois civils, si cela est techniquement faisable. |
|  | Pour les *actifs électroniques* des systèmes visés, si un mot de passe ne peut être changé dans le cas d’une authentification uniquement par mot de passe de l’accès utilisateur interactif, vérifier qu’une « TFE » a été accordée pour cette circonstance. |
|  | Pour les *actifs électroniques* des systèmes visés, si un mot de passe peut être changé dans le cas d’une authentification uniquement par mot de passe de l’accès utilisateur interactif, vérifier qu’un changement de mot de passe, au moins une fois tous les 15 mois civils, est imposé par des moyens techniques ou procéduraux. |
|  | Si une « TFE » s’applique à cet alinéa, vérifier que les mesures compensatoires identifiées à la « TFE » ont été mises en œuvre. |
| **Notes pour l’auditeur:**  Cet alinéa ne s’applique pas à l’authentification multifactorielle. | |

**Notes des auditeurs:**

**E5 Alinéa 5.7**

| **Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 5.7 | *Systèmes électroniques BES* à impact élevé et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.   *Systèmes électroniques BES* à impact moyen de *centres de contrôle* et :   1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. | Si cela est techniquement faisable :   * limiter le nombre de tentatives d’authentification infructueuses ; ou * générer des alertes après un certain nombre de tentatives d’authentification infructueuses. | Exemples non limitatifs de pièces justificatives :   * documentation des paramètres de verrouillage de compte ; ou * règles de configuration des alertes indiquant comment le système avise des personnes après un nombre défini de tentatives d’authentification infructueuses. |

**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-007-6, E4, alinéa 5.7**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus, soit :   * Pour limiter le nombre de tentatives d’authentification infructueuses, lorsque techniquement faisable ; ou * Pour générer des alertes après un certain nombre de tentatives d’authentification infructueuses. |
|  | Si le nombre de tentatives d’authentification infructueuses est limité, vérifier la configuration. |
|  | Si des alertes sont générées après un certain nombre de tentatives d’authentification infructueuses, vérifier que la configuration valide cette méthode. |
|  | Si aucune de ces méthodes n’est utilisée, vérifier qu’une « TFE » a été accordée pour cette circonstance. |
|  | Si une « TFE » s’applique à cet alinéa, vérifier que les mesures compensatoires identifiées à la « TFE » ont été mises en œuvre. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**Information supplémentaire**

**Norme de fiabilité**

Le texte complet de la norme CIP-007-6 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)