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

CIP-010-4 — Cybersécurité — Gestion des changements de configuration et analyses de vulnérabilité

***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**[[2]](#footnote-2) | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |
| **E2** | **X** | **X2** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |
| **E3** | **X** | **X2** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |
| **E4** | **X** | **X2** | **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 Québec (l’Annexe) d’une entité visée. 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 et son Annexe. 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](https://www.regie-energie.qc.ca/fr). 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](https://www.regie-energie.qc.ca/fr/entites-visees/registre-des-entites-visees-par-les-normes-de-fiabilite).

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)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Req.** | **Conclusion** | **Résumé et documentation** | **Fonctions surveillées** |
| **E1** |  |  |  |
| A1.1 |  |  |  |
| A1.2 |  |  |  |
| A1.3 |  |  |  |
| A1.4 |  |  |  |
| A1.5 |  |  |  |
| A1.6 |  |  |  |
| **E2** |  |  |  |
| A2.1 |  |  |  |
| **E3** |  |  |  |
| A3.1 |  |  |  |
| A3.2 |  |  |  |
| A3.3 |  |  |  |
| A3.4 |  |  |  |
| **E4** |  |  |  |

|  |  |
| --- | --- |
| **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-010-4) – Gestion des changements de configuration.
[*Facteur de risque de non-conformité : moyen] [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-010-4) – Gestion des changements de configuration ; d’autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

**E1 Alinéa 1.1**

| **Tableau E1 (CIP-010-4) – Gestion des changements de configuration** |
| --- |
| **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 et :1. les *EACMS* associés ;
2. les *PACS* associés ; et
3. les *PCA* associés.
 | Établir une configuration de référence, individuellement ou par groupe, qui doit comprendre les éléments suivants :* + 1. le ou les systèmes d’exploitation (y compris la version), ou tout système embarqué en l’absence de système d’exploitation indépendant ;
		2. tout logiciel commercial ou logiciel libre (y compris la version) installé intentionnellement ;
		3. tout logiciel personnalisé installé ;
		4. tout port logique accessible par le réseau ; et
		5. tout correctif de sécurité appliqué.
 | Exemples non limitatifs de pièces justificatives :* feuille de calcul indiquant les éléments de configuration de référence requis pour chaque *actif électronique*, individuellement ou par groupe ; ou
* enregistrement dans un système de gestion d’actifs indiquant les éléments de configuration de référence requis pour chaque *actif électronique*, individuellement ou par groupe.
 |

**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-010-4, E1, alinéa 1.1**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus qui comprennent l’établissement d’une configuration de référence pour chaque système visé. |
|  | Pour chaque système visé, vérifier que le ou les processus documentés comprennent collectivement tous les éléments suivants :1. le ou les systèmes d’exploitation (y compris la version), ou tout système embarqué en l’absence de système d’exploitation indépendant ;
2. tout logiciel commercial ou logiciel libre (y compris la version) installé intentionnellement ;
3. tout logiciel personnalisé installé ;
4. tout port logique accessible par le réseau ; et
5. tout correctif de sécurité appliqué.
 |
|  | Vérifier que l’entité responsable a une configuration de référence pour chaque système visé, individuellement ou par groupe, qui comprend :1. le ou les systèmes d’exploitation (y compris la version), ou tout système embarqué en l’absence de système d’exploitation indépendant ;
2. tout logiciel commercial ou logiciel libre (y compris la version) installé intentionnellement ;
3. tout logiciel personnalisé installé ;
4. tout port logique accessible par le réseau ; et
5. tout correctif de sécurité appliqué.
 |

**Notes des auditeurs :**

**E1 Alinéa 1.2**

| **Tableau E1 (CIP-010-4) – Gestion des changements de configuration** |
| --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.2 | *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.
 | Autoriser et documenter tout changement par rapport à la configuration de référence existante. | Exemples non limitatifs de pièces justificatives :* pour chaque changement, l’enregistrement dans un système de gestion des changements de la demande de changement et de l’autorisation électronique correspondante (accordée par une personne ou un groupe dûment habilité) ; ou
* documentation attestant que le changement a été effectué conformément à l’exigence.
 |

**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-010-4, E1, alinéa 1.2**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsablea documenté un ou plusieurs processus afin d’autoriser et de documenter tout changement par rapport à la configuration de référence existante. |
|  | Vérifier que l’entité responsable a autorisé et documenté tout changement par rapport à la configuration de référence existante, pour chaque système visé. |

**Notes des auditeurs :**

**E1 Alinéa 1.3**

| **Tableau E1 (CIP-010-4) – Gestion des changements de configuration** |
| --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.3 | *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 tout changement par rapport à la configuration de référence existante, mettre à jour la configuration de référence dans les 30 jours civils suivant l’exécution du changement. | Exemple non limitatif de pièce justificative : documentation de la configuration de référence avec mise à jour datée d’au plus 30 jours civils après la date d’exécution du changement. |

**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-010-4, E1, alinéa 1.3**

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

|  |  |
| --- | --- |
|  | Pour tout changement par rapport à la configuration de référence existante, vérifier que l’entité responsable a documenté un ou plusieurs processus visant à mettre à jour la configuration de référence si nécessaire dans les 30 jours civils suivant l’exécution du changement. |
|  | Pour chaque système visé et pour tout changement par rapport à la configuration de référence existante, vérifier que l’entité responsable a mis à jour la configuration de référence si nécessaire dans les 30 jours civils suivant l’exécution du changement. |

**Notes des auditeurs :**

**E1 Alinéa 1.4**

| **Tableau E1 (CIP-010-4) – Gestion des changements de configuration** |
| --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.4 | *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 tout changement par rapport à la configuration de référence existante :* + 1. avant le changement, déterminer les mécanismes de cybersécurité des normes CIP-005 et CIP-007 qui pourraient être touchés par le changement ;
		2. après le changement, vérifier que les mécanismes de cybersécurité déterminés en 1.4.1 ne sont pas dégradés ; et
		3. documenter les résultats de la vérification.
 | Exemple non limitatif de pièce justificative : liste de mécanismes de cybersécurité vérifiés ou mis à l’essai, avec résultats d’essai 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-010-4, E1, alinéa 1.4**

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

|  |  |
| --- | --- |
|  | Pour tout changement par rapport à la configuration de référence existante, vérifier que l’entité responsable a documenté un ou plusieurs processus pour :1. déterminer, avant le changement, les mécanismes de cybersécurité des normes CIP-005 et CIP-007 qui pourraient être touchés par le changement ;
2. vérifier, après le changement, que les mécanismes de cybersécurité déterminés en 1.4.1 ne sont pas dégradés et ;
3. documenter les résultats de la vérification.
 |
|  | Pour chaque système visé et pour chaque changement par rapport à la configuration de référence existante, vérifier que :1. avant le changement, l’entité responsable a déterminé les mécanismes de cybersécurité des normes CIP-005 et CIP-007 qui pourraient être touchés par le changement ;
2. à la suite du changement, l’entité responsablea vérifié que les mécanismes de cybersécurité déterminés en 1, ci-dessus, ne sont pas dégradés et ;
3. l’entité responsablea documenté les résultats de la vérification requise au point 2 ci-dessus.
 |

**Notes des auditeurs :**

**E1 Alinéa 1.5**

| **Tableau E1 (CIP-010-4) – Gestion des changements de configuration** |
| --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.5 | *Systèmes électroniques BES* à impact élevé. | Pour chaque changement par rapport à la configuration de référence existante, dans la mesure où c’est techniquement faisable :* + 1. avant de mettre en œuvre un changement dans l’environnement de production, mettre à l’essai le changement dans un environnement d’essai ou mettre à l’essai le changement dans un environnement de production où l’essai est effectué d’une manière qui réduit au minimum les effets adverses, en simulant la configuration de référence de manière à s’assurer que les mécanismes de cybersécurité des normes CIP-005 et CIP-007 ne sont pas dégradés ; et
		2. documenter les résultats des essais et, si un environnement d’essai a été utilisé, les différences entre celui-ci et l’environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d’essai et de production.
 | Exemples non limitatifs de pièces justificatives : liste des mécanismes de cybersécurité mis à l’essai avec résultats d’essai concluants, liste de différences entre les environnements d’essai et de production et description des mesures visant à tenir compte des différences de fonctionnement, y compris la date de l’essai. |

**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-010-4, E1, alinéa 1.5**

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

|  |  |
| --- | --- |
|  | Pour tout changement par rapport à la configuration de référence existante, vérifier que l’entité responsable a documenté un ou plusieurs processus qui comprennent :1. avant de mettre en œuvre un changement dans l’environnement de production, une mise à l’essai du changement dans un environnement d’essai ou une mise à l’essai du changement dans un environnement de production où l’essai est effectué d’une manière qui réduit au minimum les effets adverses, en simulant la configuration de référence de manière à s’assurer que les mécanismes de cybersécurité des normes CIP-005 et CIP-007 ne sont pas dégradés ; et
2. la documentation des résultats des essais et, si un environnement d’essai a été utilisé, les différences entre celui-ci et l’environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d’essai et de production.
 |
|  | Pour chaque système visé et pour chaque changement par rapport à la configuration de référence existante, avant de mettre en œuvre un changement dans l’environnement de production où une exception pour raison technique (« TFE ») n’a pas couvert cette situation, vérifier que :* l’entité responsable a mis à l’essai les changements dans un environnement d’essai qui simulait la configuration de référence de manière à s’assurer que les mécanismes de cybersécurité des normes CIP-005 et CIP-007 n’ont pas étés dégradés en raison de ces changements ; ou
* l’entité responsable a mis à l’essai les changements dans un environnement de production où l’essai a été effectué d’une manière qui a réduit au minimum les effets adverses, de manière à s’assurer que les mécanismes de cybersécurité des normes CIP-005 et CIP-007 n’ont pas étés dégradés en raison de ces changements.
 |
|  | Pour chaque système visé et pour chaque changement par rapport à la configuration de référence existante, si cela est techniquement possible, vérifier que :1. l’entité responsable a documenté les résultats des essais ; et
2. si un environnement d’essai a été utilisé, l’entité responsable a documenté les différences entre celui-ci et l’environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d’essai et de production.
 |
|  | Si une « TFE » s’applique à cette exigence, vérifier que les mesures compensatoires identifiées à la « TFE » ont été mises en œuvre. |
| **Notes pour l’auditeur :** L’entité responsable peut tenir à jour un document décrivant les différences entre l’environnement d’essai et l’environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d’essai et de production, plutôt que de documenter ces différences pour chaque changement. Si tel est le cas, ce document devrait être mentionné à la documentation visant les changements, et peut être passé en revue par l’équipe d’audit dans le cadre de la documentation en lien avec les changements. |

**Notes des auditeurs :**

**E1 Alinéa 1.6**

| **Tableau E1 (CIP-010-4) – Gestion des changements de configuration** |
| --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.6 | *Systèmes électroniques BES* à impact élevé et :1. les *EACMS* associés ; et
2. les *PACS* associés.

*Systèmes électroniques BES* à impact moyen et :1. les *EACMS* associés ; et
2. les *PACS* associés.

Remarque : La mise en œuvre d’un plan n’oblige pas l’entité responsable à renégocier ou à résilier des contrats existants (y compris les modifications aux ententes-cadres ou les bons de commande). En outre, la partie 1.6 ne s’étend pas : 1) aux modalités mêmes d’un contrat d’approvisionnement ; et2) à l’exécution et au respect du contrat par le fournisseur. | Avant tout changement touchant les éléments de la configuration de référence spécifiés aux alinéas 1.1.1, 1.1.2 et 1.1.5 par rapport à la configuration existante, dans la mesure où la source d’un logiciel met les méthodes appropriées à la disposition de l’entité responsable :* + 1. vérifier l’identité de la source du logiciel ; et
		2. vérifier l’intégrité du logiciel obtenu de la source du logiciel.
 | Exemples non limitatifs de pièces justificatives : enregistrement d’une demande de changement qui atteste que l’identité de la source du logiciel et l’intégrité du logiciel ont été vérifiées avant le changement à la configuration de référence ; ou processus qui documente les mécanismes en place pour assurer la vérification automatique de l’identité de la source du logiciel et de l’intégrité du logiciel. |

**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-010-4, E1, alinéa 1.6**

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

|  |  |
| --- | --- |
|  | Pour les changements touchant les éléments de la configuration de référence spécifiés aux alinéas 1.1.1, 1.1.2 et 1.1.5 par rapport à la configuration existante, vérifier que l’entité responsable a documenté un ou plusieurs processus qui comprennent :1. la vérification de l’identité de la source du logiciel ; et
2. la vérification de l’intégrité du logiciel obtenu de la source du logiciel.
 |
|  | Vérifier que, pour chaque système visé, avant chaque changement touchant les éléments de la configuration de référence spécifiés aux alinéas 1.1.1, 1.1.2 et 1.1.5 par rapport à la configuration existante :* l’entité responsable a vérifié l’identité de la source du logiciel ; ou
* l’entité responsable a documenté qu’une méthode pour vérifier l’identité de la source du logiciel n'est pas disponible pour l’entité responsable à partir de la source du logiciel.
 |
|  | L’alinéa 1.6 n'exige pas que l’entité responsable vérifie l’identité de la source du logiciel lorsqu’aucune méthode n’est disponible pour le faire à partir de la source du logiciel. Si tel est le cas, vérifier qu’aucune méthode n’est disponible pour l’entité responsable à partir de la source du logiciel pour vérifier l’identité de la source du logiciel. |
|  | Vérifier que, pour chaque système visé, avant chaque changement touchant les éléments de la configuration de référence spécifiés aux alinéas 1.1.1, 1.1.2 et 1.1.5 par rapport à la configuration existante :* l’entité responsable a vérifié l’intégrité du logiciel obtenu à partir de la source du logiciel ; ou
* l’entité responsable a documenté qu’une méthode pour vérifier l’intégrité du logiciel obtenu à partir de la source du logiciel n’est pas disponible pour l’entité responsable à partir de la source du logiciel.
 |
|  | L’alinéa 1.6 n'exige pas que l’entité responsable vérifie l’intégrité du logiciel lorsqu’aucune méthode n’est disponible pour le faire à partir de la source du logiciel. Si tel est le cas, vérifier qu’aucune méthode n’est disponible pour l’entité responsable à partir de la source du logiciel pour vérifier l’intégrité du logiciel. |
| **Notes pour l’auditeur :** Si l’identité de la source du logiciel ne peut pas être vérifiée, il ne sera pas possible de vérifier l’intégrité du logiciel obtenu à partir de la source du logiciel. Dans ce cas, la documentation portant sur l’incapacité à vérifier l’identité de la source du logiciel peut également servir à documenter l’incapacité à vérifier l’intégrité du logiciel. |

**Notes des auditeurs :**

**E2 Documentation et preuve 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-010-4) – Surveillance de la configuration.
*[Facteur de risque de non-conformité : moyen] [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 E2 (CIP-010-4) – Surveillance de la configuration ; d’autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau*.*

**E2 Alinéa 2.1**

| **Tableau E2 (CIP-010-4) – Surveillance de la configuration** |
| --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.1 | *Systèmes électroniques BES* à impact élevé et :1. les *EACMS* associés ; et
2. les *PCA* associés.
 | Au moins une fois tous les 35 jours civils, vérifier s’il y a eu des changements à la configuration de référence (décrite à l’alinéa 1.1 de l’exigence E1). Documenter tout changement non autorisé détecté et faire enquête. | Exemples non limitatifs de pièces justificatives : registres d’un système de surveillance de configuration et dossiers d’enquête pour tout changement non autorisé détecté. |

**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-010-4, E2, alinéa 2.1**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus afin de vérifier au moins une fois tous les 35 jours civils s’il y a eu des changements dans la configuration de référence (décrite à l’alinéa 1.1 de l’exigence E1). |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus afin de documenter tout changement non autorisé détecté et de faire enquête. |
|  | Pour chaque système visé, vérifier que l’entité responsable a vérifié au moins une fois tous les 35 jours civils s’il y a eu des changements dans la configuration de référence (décrite à l’alinéa 1.1 de l’exigence E1). |
|  | Pour chaque système visé, vérifier que tous les changements non autorisés détectés ont été documentés et ont fait l’objet d’une enquête. |

**Notes des auditeurs :**

**E3 Documentation et preuve 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-010-4) – Analyses de vulnérabilité. *[Facteur de risque de non-conformité : moyen] [Horizon : planification à long terme et planification de l’exploitation]*
2. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-010-4) – Analyses de vulnérabilité ; d’autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau*.*

**E3 Alinéa 3.1**

| **Tableau E3 (CIP-010-4) – Analyses de vulnérabilité** |
| --- |
| **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.
 | Au moins tous les 15 mois civils, effectuer une analyse de vulnérabilité sur papier ou active. | Exemples non limitatifs de pièces justificatives :* document indiquant la date de l’analyse (effectuée au moins une fois tous les 15 mois civils), les mécanismes évalués pour chaque *système électronique BES* et la méthode d’analyse ; ou
* document indiquant la date de l’analyse et le résultat produit par tout outil utilisé pour l’analyse.
 |

**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-010-4, E3, alinéa 3.1**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus afin d’effectuer une analyse de vulnérabilité sur papier ou active au moins une fois tous les 15 mois civils. |
|  | Pour chaque système visé, vérifier que l’entité responsable a effectué une analyse de vulnérabilité sur papier ou active au moins une fois tous les 15 mois civils. |

**Notes des auditeurs :**

**E3 Alinéa 3.2**

| **Tableau E3 (CIP-010-4) – Analyses de vulnérabilité** |
| --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.2 | *Systèmes électroniques BES* à impact élevé. | Au moins une fois tous les 36 mois civils, dans la mesure où c’est techniquement faisable :* + 1. effectuer une analyse de vulnérabilité active dans un environnement d’essai, ou effectuer une analyse de vulnérabilité active dans un environnement de production où l’essai est réalisé d’une manière qui réduit au minimum les effets adverses, en simulant la configuration de référence du *système électronique BES* dans un environnement de production ; et
		2. documenter les résultats des essais et, si un environnement d’essai a été utilisé, les différences entre celui-ci et l’environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d’essai et de production.
 | Exemples non limitatifs de pièces justificatives : document indiquant la date de l’analyse (effectuée au moins une fois tous les 36 mois civils), résultat produit par les outils utilisés pour effectuer l’analyse et liste des différences entre les environnements de production et d’essai, avec explications sur la prise en compte des différences dans l’analyse. |

**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-010-4, E3, alinéa 3.2**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus pour :1. effectuer une analyse de vulnérabilité active dans un environnement d’essai, ou effectuer une évaluation de vulnérabilité active dans un environnement de production où l’essai est réalisé d’une manière qui réduit au minimum les effets adverses, en simulant la configuration de référence du *système électronique BES* dans un environnement de production ; et
2. documenter les résultats des essais et, si un environnement d’essai a été utilisé, les différences entre celui-ci et l’environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d’essai et de production.
 |
|  | Pour chaque système visé, une analyse de vulnérabilité active était-elle techniquement faisable? * Si oui, vérifier que :
	+ Une analyse de vulnérabilité active a été réalisée au moins une fois tous les 36 mois civils, conformément à 3.2.1 ; et
	+ Les résultats des tests sont documentés, conformément au 3.2.2.
* Si non, vérifier que les mesures compensatoires identifiées à la « TFE » ont été mises en œuvre.
 |

**Notes des auditeurs :**

**E3 Alinéa 3.3**

| **Tableau E3 (CIP-010-4) – Analyses de vulnérabilité** |
| --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.3 | *Systèmes électroniques BES* à impact élevé et :1. les *EACMS* associés ; et
2. les *PCA* associés.
 | Avant d’ajouter un nouvel *actif électronique* visé à un environnement de production, effectuer une analyse de vulnérabilité active du nouvel *actif électronique*, sauf dans des *circonstances CIP exceptionnelles* ou pour un remplacement d’un *actif électronique* existant par un équivalent dont la configuration de référence simule celle de l’*actif électronique* remplacé ou d’un autre *actif électronique* existant. | Exemples non limitatifs de pièces justificatives : document indiquant la date de l’analyse (effectuée avant la mise en service du nouvel *actif électronique*) et le résultat produit par les outils utilisés pour l’analyse. |

**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-010-4, E3, alinéa 3.3**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsablea documenté un ou plusieurs processus pour effectuer une analyse de vulnérabilité active du nouvel *actif électronique* avant d’ajouter un nouvel *actif électronique* visé à un environnement de production, sauf dans des *circonstances CIP exceptionnelles* ou pour un remplacement d’un *actif électronique* existant par un équivalent dont la configuration de référence simule celle de l’*actif électronique* remplacé ou d’un autre *actif électronique* existant. |
|  | Pour chaque système visé, un nouvel *actif électronique* a-t-il été ajouté à un environnement de production? Si oui, vérifier qu'une analyse de vulnérabilité active du nouvel *actif électronique* a été effectuée avant de l’ajouter à un environnement de production, sauf dans des *circonstances CIP exceptionnelles* ou pour un remplacement d’un *actif électronique* existant par un équivalent dont la configuration de référence simule celle de l’*actif électronique* remplacé ou d’un autre *actif électronique* existant. |
|  | Si l’entité responsable a répondu à des *circonstances CIP exceptionnelles*, vérifier qu’elle a respecté toute politique de cybersécurité applicable. |
| **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 :**

**E3 Alinéa 3.4**

| **Tableau E3 (CIP-010-4) – Analyses de vulnérabilité** |
| --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.4 | *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.
 | Documenter les résultats des analyses effectuées conformément aux alinéas 3.1, 3.2 et 3.3 ainsi que le plan d’action visant à corriger ou à atténuer les vulnérabilités constatées lors des analyses, en précisant la date prévue d’achèvement du plan d’action et l’état d’exécution de toute mesure de correction ou d’atténuation. | Exemples non limitatifs de pièces justificatives : document donnant les résultats de l’examen ou de l’analyse, liste des mesures à prendre, dates proposées d’achèvement du plan d’action et dossier de l’état d’exécution des mesures à prendre (procès-verbaux de réunion d’étape, mises à jour dans un système d’ordres de travail, suivi des mesures au moyen d’une feuille de calcul, 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-010-4, E3, alinéa 3.4**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs processus afin de documenter les résultats des analyses effectuées conformément aux alinéas 3.1, 3.2 et 3.3 ainsi que le plan d’action visant à corriger ou à atténuer les vulnérabilités constatées lors des analyses, en précisant la date prévue d’achèvement du plan d’action et l’état d’exécution de toute mesure de correction ou d’atténuation. |
|  | Pour chaque système visé, vérifier que les résultats de chaque analyse effectuée conformément aux alinéas 3.1, 3.2 et 3.3 ont été documentés. |
|  | Pour chaque analyse de chaque système visé effectuée conformément aux alinéas 3.1, 3.2 et 3.3, est-ce que des vulnérabilités ont été constatées?Si oui, vérifier les éléments suivants :1. un plan d’action visant à corriger ou à atténuer les vulnérabilités constatées a été élaboré ou modifié ;
2. le plan d’action comporte une date prévue d’achèvement ;
3. le plan d’action comporte l’état d’exécution de toute mesure de correction ou d’atténuation ;
4. l’état du plan d’action, si la date prévue d’achèvement est dépassée ; et
5. l’achèvement du plan d’action, si le plan d’action est complété.
 |

**Notes des auditeurs :**

**E4 Documentation et preuve à l’appui**

1. Chaque entité responsable, pour ses *systèmes électroniques BES* à impact moyen et élevé ainsi que les *actifs électroniques protégés* connexes, doit mettre en œuvre (sauf dans des *circonstances CIP* *exceptionnelles*) un ou plusieurs plans documentés concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles* ; ces plans doivent être conformes aux sections de l’annexe 1.
*[Facteur de risque de non-conformité : moyen] [Horizon : planification à long terme et planification de l’exploitation]*
2. Les pièces justificatives doivent comprendre chacun des plans documentés qui concernent les *actifs électroniques temporaires* et les *supports de stockage amovibles* et qui, collectivement, couvrent toutes les sections applicables de l’annexe 1 ; d’autres pièces justificatives doivent attester la mise en œuvre de ces plans. D’autres exemples de pièces justificatives pour les différentes sections sont présentés à l’annexe 2. Si une entité responsable n’utilise pas d’*actifs électroniques temporaires* ni de *supports de stockage amovibles*, les pièces justificatives appropriées peuvent comprendre, sans limitation, une déclaration, une politique ou tout autre document affirmant que l’entité responsable n’utilise pas d’*actifs électroniques temporaires* ou de *supports de stockage amovibles.*

**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-010-4, E4**

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

|  |
| --- |
| **Section 1. Pour les *actifs électroniques temporaires* gérés par l’entité responsable :** |
|  | Vérifier que l’entité responsable a documenté au moins un plan, tel qu’indiqué à l’annexe 1, pour les *actifs électroniques temporaires*, qui comporte :1. la gestion des *actifs électroniques temporaires* ;
2. les autorisations relatives aux *actifs électroniques temporaires* ;
3. l’atténuation du risque lié aux vulnérabilités logicielles ;
4. l’atténuation du risque lié à l’introduction de programmes malveillants ; et
5. l’atténuation du risque lié aux utilisations non autorisées.
 |
|  | Vérifier que l’entité responsable a mis en œuvre son ou ses plans de gestion des *actifs électroniques temporaires* individuels ou par groupe : (1) en permanence, afin d’assurer la conformité aux exigences pertinentes en tout moment, (2) à la demande, en appliquant les exigences pertinentes avant d’établir la connexion à un *système électronique BES*, ou (3) selon une combinaison des moyens (1) et (2) ci-dessus. |
|  | Pour chaque *actif électronique temporaire* ou groupe d’*actifs électroniques temporaires*, vérifier que l’entité responsable autorise :1. les utilisateurs, individuellement, par groupe ou par rôle ;
2. les emplacements, individuellement ou par groupe ; et
3. les utilisations, qui doivent être limitées aux actions nécessaires pour assurer les fonctions opérationnelles.
 |
|  | Vérifier que l’entité responsable a mis en œuvre un ou plusieurs des moyens suivants pour réaliser l’objectif d’atténuer le risque lié aux vulnérabilités présentées par des logiciels sans correctifs dans l’*actif électronique temporaire* (selon la capacité de ce dernier) :* application de correctifs, manuellement ou par mises à jour systématiques ;
* systèmes d’exploitation et logiciels exécutables uniquement à partir de supports non inscriptibles ;
* renforcement du système d’exploitation ; ou
* autres moyens d’atténuer le risque lié aux vulnérabilités logicielles.

Si un *actif électronique temporaire* n’a pas la capacité de mettre complètement en œuvre un des moyens précédents, vérifier les capacités de l’*actif électronique temporaire* et la mise en œuvre de ses capacités selon l’exigence. |
|  | Vérifier que l’entité responsable a mis en œuvre un ou plusieurs des moyens suivants pour réaliser l’objectif d’atténuer le risque lié à l’introduction de programmes malveillants dans l’*actif électronique temporaire* (selon la capacité de ce dernier) :* logiciel antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code ;
* liste blanche d’application ; ou
* autres moyens d’atténuer le risque lié à l’introduction de programmes malveillants.

Si un *actif électronique temporaire* n’a pas la capacité de mettre complètement en œuvre un des moyens précédents, vérifier les capacités de l’*actif électronique temporaire* et la mise en œuvre de ses capacités selon l’exigence. |
|  | Vérifier que l’entité responsable a mis en œuvre un ou plusieurs des moyens suivants pour réaliser l’objectif d’atténuer le risque lié aux utilisations non autorisées d’*actifs électroniques temporaires* :* restriction de l’accès physique ;
* cryptage de disque intégral avec authentification ;
* authentification multifactorielle ; ou
* autres moyens d’atténuer le risque lié aux utilisations non autorisées.
 |

|  |
| --- |
| **Section 2. Pour les *actifs électroniques temporaires* gérés par une tierce partie autre que l’entité responsable :** |
|  | Vérifier que l’entité responsable a documenté au moins un plan, tel qu’indiqué à l’annexe 1, pour les *actifs électroniques temporaires* gérés par une tierce partie autre que l’entité responsable, qui comporte :1. l’atténuation du risque lié aux vulnérabilités logicielles ;
2. l’atténuation du risque lié à l’introduction de programmes malveillants ; et
3. la détermination si d’autres mesures d’atténuation sont nécessaires, le cas échéant.
 |
|  | Vérifier que l’entité responsable a mis en œuvre un ou plusieurs des moyens suivants pour réaliser l’objectif d’atténuer le risque lié aux vulnérabilités logicielles dans l’*actif électronique temporaire* (selon la capacité de ce dernier) :* examen des correctifs de sécurité installés ;
* examen de la procédure d’application des correctifs par la tierce partie ;
* examen d’autres mesures d’atténuation du risque lié aux vulnérabilités logicielles adoptées par la tierce partie ; ou
* autres moyens d’atténuer le risque lié aux vulnérabilités logicielles.

Si un *actif électronique temporaire* n’a pas la capacité de mettre complètement en œuvre un des moyens précédents, vérifier les capacités de l’*actif électronique temporaire* et la mise en œuvre de ses capacités selon l’exigence. |
|  | Vérifier que l’entité responsable a mis en œuvre un ou plusieurs des moyens suivants pour réaliser l’objectif d’atténuer le risque lié à l’introduction de programmes malveillants dans l’*actif électronique temporaire* (selon la capacité de ce dernier) :* examen du degré de maintien à jour de l’antivirus ;
* examen de la procédure de mise à jour de l’antivirus adoptée par la tierce partie ;
* examen de l’utilisation par la tierce partie de listes blanches d’applications ;
* examen de l’utilisation de systèmes d’exploitation et de logiciels exécutables uniquement à partir de supports non inscriptibles ;
* examen des mesures de renforcement du système d’exploitation adoptées par la tierce partie ; ou
* autres moyens d’atténuer le risque lié aux programmes malveillants.

Si un *actif électronique temporaire* n’a pas la capacité de mettre complètement en œuvre un des moyens précédents, vérifier les capacités de l’*actif électronique temporaire* et la mise en œuvre de ses capacités selon l’exigence. |
|  | Pour tout moyen d’atténuation du risque lié aux vulnérabilités logicielles ou à l’introduction de programmes malveillants mis en œuvre conformément aux alinéas 2.1 et 2.2 :1. Vérifier que l’entité responsable a déterminé si d’autres mesures d’atténuation supplémentaires sont nécessaires.
2. Si des mesures d’atténuation supplémentaires étaient nécessaires, vérifier qu’elles ont été mises en œuvre avant de connecter l’*actif électronique temporaire*.
 |

|  |
| --- |
| **Section 3. Pour les *supports de stockage amovibles* :** |
|  | Vérifier que l’entité responsable a documenté au moins un plan, tel qu’indiqué à l’annexe 1, pour les *supports de stockage amovibles*, qui comporte :1. l’autorisation relatives aux *supports de stockage amovibles* ;
2. l’atténuation du risque lié aux programmes malveillants.
 |
|  | Pour chaque *support de stockage amovible* ou groupe de *support de stockage amovible*, vérifier que l’entité responsable a autorisé :1. les utilisateurs, individuellement, par groupe ou par rôle ; ou
2. les emplacements, individuellement ou par groupe.
 |
|  | Vérifier que l’entité responsable a mis en œuvre un ou plusieurs des moyens suivants pour réaliser l’objectif d’atténuer le risque lié à l’introduction de programmes malveillants dans des *systèmes électroniques BES* à impact élevé ou moyen et dans les *actifs électroniques protégés* connexes :1. prendre des mesures pour détecter les programmes malveillants sur les *supports de stockage amovibles* au moyen d’un *actif électronique* autre qu’un *système électronique BES* ou que des *actifs électroniques protégés* ; et
2. neutraliser la menace de programmes malveillants détectés sur des *supports de stockage amovibles* avant de connecter ces supports à un *système électronique BES* à impact moyen ou élevé ou à des *actifs électroniques protégés* connexes.
 |

**Notes des auditeurs :**

**Information supplémentaire**

**Norme de fiabilité**

Le texte complet de la norme CIP-010-4 peut être consulté sur le site internet de la Régie de l’énergie, à la section [Entités visées - Normes de fiabilité](https://www.regie-energie.qc.ca/fr/entites-visees).



**Historique des révisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Réviseurs** | **Description de la révision** |
| 1 | Novembre 2023 | Document initial | Document créé à partir du formulaire « RSAW » de la NERC |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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)
2. La norme CIP-010-4 est applicable aux *distributeurs* qui possèdent certains systèmes de délestage de *charge* en sous-fréquence (DSF) ou en sous-tension (DST), des *automatismes de réseau* (*RAS*), des *systèmes de protection*, ou des *chemins de démarrage*. Consulter la section 4, Applicabilité de la norme CIP-010-4 pour des informations supplémentaires. [↑](#footnote-ref-2)