

A. Introduction

1. **Titre :** Cybersécurité — Gestion des changements de configuration et analyses de vulnérabilité
2. **Numéro :** CIP-010-4

3. **Objet :** Prévenir et détecter les changements non autorisés aux *systèmes électroniques BES* au moyen d'exigences relatives à la gestion des changements de configuration et aux analyses de vulnérabilité, afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le *système de production-transport d'électricité (BES)*.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1. Responsable de l'équilibrage

4.1.2. Distributeur qui possède un ou plusieurs des systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :

4.1.2.1. Système de délestage de *charge* en sous-fréquence (DSF) ou en sous-tension (DST) qui :

4.1.2.1.1. fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale* ; et

4.1.2.1.2. effectue des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.1.2.2. *Automatisme de réseau (RAS)* visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale*.

4.1.2.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale*.

4.1.2.4. *Chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des prochains groupes de production à démarrer.

4.1.3. Exploitant d'installation de production

4.1.4. Propriétaire d'installation de production

4.1.5. Coordonnateur de la fiabilité

4.1.6. Exploitant de réseau de transport

4.1.7. Propriétaire d'installation de transport

4.2. Installations : Dans le contexte de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par les exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1. Distributeur : Chacun des systèmes, *installations* et équipements suivants détenus par le *distributeur* pour la protection ou la remise en charge du *BES* :

4.2.1.1. Système de DSF ou de DST qui :

4.2.1.1.1. fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale* ; et

4.2.1.1.2. effectue des délestages de *charge* automatiques de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.2.1.2. Automatisation de réseau (RAS) visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale*.

4.2.1.3. Système de protection de réseau de transport (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale*.

4.2.1.4. Chemin de démarrage et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des prochains groupes de production à démarrer.

4.2.2. Entités responsables indiquées en 4.1, sauf les distributeurs : Toutes les *installations* du *BES*.

4.2.3. Exemptions : Sont exemptés de la norme CIP-010-4 :

4.2.3.1. Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire.

4.2.3.2. Les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électronique* distincts.

4.2.3.3. Les systèmes, structures et composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54.

4.2.3.4. Dans le cas des *distributeurs*, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus.

4.2.3.5. Les entités responsables qui ont déterminé n'avoir aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation de la norme CIP-002.

5. Date d'entrée en vigueur : Voir le plan de mise en œuvre du projet 2019-03.

6. Contexte :

La norme CIP-010 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES* ainsi qu'un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui couvrent tous les alinéas applicables du tableau [référence au tableau]. » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », dans la mesure où la compréhension relève du bon sens. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont des exemples qui figurent dans les normes. La mise en œuvre complète des *normes de fiabilité* CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel concernant plusieurs *systèmes électroniques BES*.

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés ; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes de DSF et de DST. Ce seuil particulier de 300 MW pour les systèmes de DSF et de DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes de DST et de DSF, qui constituent des efforts de dernier recours pour sauver le *BES*. Un examen des tolérances des systèmes de DSF définies dans les *normes de fiabilité* régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de

300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes de DSF.

Colonne « **Systèmes visés** » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. L'équipe de rédaction (SDT) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus d'inventaire et de catégorisation de la norme CIP-002.
- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002.
- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS)** – Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification et systèmes de surveillance de registre d'événements et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès physiques* associés à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.
- **Actifs électroniques protégés (PCA)** – Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

- E1.** 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].
- M1.** 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.

| Tableau E1 (CIP-010-4) – Gestion des changements de configuration | | | |
|---|---|--|---|
| Alinéa | Systèmes visés | Exigences | Mesures |
| 1.1 | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. | <p>Établir une configuration de référence, individuellement ou par groupe, qui doit comprendre les éléments suivants :</p> <ol style="list-style-type: none"> 1.1.1. le ou les systèmes d’exploitation (y compris la version), ou tout système embarqué en l’absence de système d’exploitation indépendant ; 1.1.2. tout logiciel commercial ou logiciel libre (y compris la version) installé intentionnellement ; 1.1.3. tout logiciel personnalisé installé ; 1.1.4. tout port logique accessible par le réseau ; et 1.1.5. tout correctif de sécurité appliqué. | <p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • feuille de calcul indiquant les éléments de configuration de référence requis pour chaque <i>actif électronique</i>, individuellement ou par groupe ; ou • enregistrement dans un système de gestion d’actifs indiquant les éléments de configuration de référence requis pour chaque <i>actif électronique</i>, individuellement ou par groupe. |

| Tableau E1 (CIP-010-4) – Gestion des changements de configuration | | | |
|---|---|--|---|
| Alinéa | Systèmes visés | Exigences | Mesures |
| 1.2 | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. | <p>Autoriser et documenter tout changement par rapport à la configuration de référence existante.</p> | <p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • 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. |
| 1.3 | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. | <p>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.</p> | <p>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.</p> |

| Tableau E1 (CIP-010-4) – Gestion des changements de configuration | | | |
|---|---|---|---|
| Alinéa | Systèmes visés | Exigences | Mesures |
| 1.4 | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. | <p>Pour tout changement par rapport à la configuration de référence existante :</p> <ol style="list-style-type: none"> 1.4.1. avant le changement, déterminer les mécanismes de cybersécurité des normes CIP-005 et CIP-007 qui pourraient être touchés par le changement ; 1.4.2. après le changement, vérifier que les mécanismes de cybersécurité déterminés en 1.4.1 ne sont pas dégradés ; et 1.4.3. documenter les résultats de la vérification. | <p>Exemple non limitatif de pièce justificative : liste de mécanismes de cybersécurité vérifiés ou mis à l'essai, avec résultats d'essai datés.</p> |

| Tableau E1 (CIP-010-4) – Gestion des changements de configuration | | | |
|---|---|---|---|
| Alinéa | Systèmes visés | Exigences | Mesures |
| 1.5 | <i>Systèmes électroniques BES</i> à impact élevé. | <p>Pour chaque changement par rapport à la configuration de référence existante, dans la mesure où c'est techniquement faisable :</p> <p>1.5.1. 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</p> <p>1.5.2. 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.</p> | <p>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.</p> |

| Tableau E1 (CIP-010-4) – Gestion des changements de configuration | | | |
|---|---|--|---|
| Alinéa | Systèmes visés | Exigences | Mesures |
| 1.6 | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; et 2. les <i>PACS</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; et 2. les <i>PACS</i> associés. <p>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 ; et 2) à l'exécution et au respect du contrat par le fournisseur.</p> | <p>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 :</p> <ol style="list-style-type: none"> 1.6.1. vérifier l'identité de la source du logiciel ; et 1.6.2. vérifier l'intégrité du logiciel obtenu de la source du logiciel. | <p>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.</p> |

- E2.** 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].
- M2.** 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.

| Tableau E2 (CIP-010-4) – Surveillance de la configuration | | | |
|---|---|--|--|
| Alinéa | Systèmes visés | Exigences | Mesures |
| 2.1 | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; et 2. les <i>PCA</i> associés. | <p>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.</p> | <p>Exemples non limitatifs de pièces justificatives : registres d'un système de surveillance de configuration et dossiers d'enquête pour tout changement non autorisé détecté.</p> |

E3. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-010-3) – Analyses de vulnérabilité.

[Facteur de risque de non-conformité : moyen] [Horizon : planification à long terme et planification de l'exploitation]

M3. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-010-3) – Analyses de vulnérabilité ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

| Tableau E3 (CIP-010-4) – Analyses de vulnérabilité | | | |
|--|---|---|---|
| Alinéa | Systèmes visés | Exigences | Mesures |
| 3.1 | <p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. | <p>Au moins tous les 15 mois civils, effectuer une analyse de vulnérabilité sur papier ou active.</p> | <p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • document indiquant la date de l'analyse (effectuée au moins une fois tous les 15 mois civils), les mécanismes évalués pour chaque <i>système électronique BES</i> et la méthode d'analyse ; ou • document indiquant la date de l'analyse et le résultat produit par tout outil utilisé pour l'analyse. |

| Tableau E3 (CIP-010-4) – Analyses de vulnérabilité | | | |
|--|---|--|---|
| Alinéa | Systèmes visés | Exigences | Mesures |
| 3.2 | <i>Systèmes électroniques BES</i> à impact élevé. | <p>Au moins une fois tous les 36 mois civils, dans la mesure où c’est techniquement faisable :</p> <p>3.2.1 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 <i>système électronique BES</i> dans un environnement de production ; et</p> <p>3.2.2 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.</p> | <p>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.</p> |

| Tableau E3 (CIP-010-4) – Analyses de vulnérabilité | | | |
|--|---|---|--|
| Alinéa | Systèmes visés | Exigences | Mesures |
| 3.3 | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; et 2. les <i>PCA</i> associés. | <p>Avant d'ajouter un nouvel <i>actif électronique</i> visé à un environnement de production, effectuer une analyse de vulnérabilité active du nouvel <i>actif électronique</i>, sauf dans des <i>circonstances CIP exceptionnelles</i> ou pour un remplacement d'un <i>actif électronique</i> existant par un équivalent dont la configuration de référence simule celle de l'<i>actif électronique</i> remplacé ou d'un autre <i>actif électronique</i> existant.</p> | <p>Exemples non limitatifs de pièces justificatives : document indiquant la date de l'analyse (effectuée avant la mise en service du nouvel <i>actif électronique</i>) et le résultat produit par les outils utilisés pour l'analyse.</p> |
| 3.4 | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. | <p>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.</p> | <p>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.).</p> |

- E4.** 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*]
- M4.** 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*.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Le terme « *responsable des mesures pour assurer la conformité* » (CEA) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les *normes de fiabilité* obligatoires et exécutoires de la NERC dans leurs territoires respectifs.

1.2. Conservation des pièces justificatives

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives attestant sa conformité pendant la période complète écoulée depuis le dernier audit.

L'entité visée doit conserver les données ou pièces justificatives attestant sa conformité selon les modalités indiquées ci-après, à moins que son CEA lui demande de conserver certaines pièces justificatives plus longtemps dans le cadre d'une enquête.

- Chaque entité visée doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité visée est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les dossiers de l'audit le plus récent ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Programme de surveillance de la conformité et d'application des normes

Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance de la conformité et d'application des normes » désigne la liste des processus qui serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité avec la *norme de fiabilité*.

Niveaux de gravité de la non-conformité (VSL)

| Ex. | Niveaux de gravité de la non-conformité | | | |
|-----|--|---|--|---|
| | VSL faible | VSL modéré | VSL élevé | VSL critique |
| E1. | L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprennent seulement quatre des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1) | L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprennent seulement trois des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1) | <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprennent seulement deux des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1)</p> <p>OU</p> <p>L'entité responsable a un processus conforme à l'alinéa 1.6 pour vérifier l'identité de la source du logiciel (1.6.1), mais n'a pas de processus conforme à l'alinéa 1.6 pour vérifier l'intégrité du logiciel obtenu de la source du logiciel alors que la méthode appropriée est mise à la disposition de l'entité responsable par la source du logiciel (1.6.2).</p> | <p>L'entité responsable n'a documenté ou mis en œuvre aucun processus de gestion des changements de configuration. (E1)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprennent seulement un des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1)</p> <p>OU</p> <p>L'entité responsable n'a pas de processus qui exige l'autorisation et la documentation des changements par rapport à la configuration de référence existante. (1.2)</p> <p>OU</p> <p>L'entité responsable n'a pas de processus pour mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution de changements par rapport à la configuration de référence existante. (1.3)</p> <p>OU</p> |

| Ex. | Niveaux de gravité de la non-conformité | | | |
|-----|---|------------|-----------|--|
| | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | | <p>L'entité responsable n'a pas de processus pour déterminer les mécanismes de sécurité exigés par les normes CIP-005 et CIP-007 qui pourraient être touchés par des changements par rapport à la configuration de référence existante. (1.4.1)</p> <p>OU</p> <p>L'entité responsable a un ou des processus pour déterminer les mécanismes de sécurité exigés par les normes CIP-005 et CIP-007 qui pourraient être touchés par des changements par rapport à la configuration de référence existante, mais elle n'a pas vérifié et documenté que les mécanismes exigés n'étaient pas dégradés par suite du changement. (1.4.2 et 1.4.3)</p> <p>OU</p> <p>L'entité responsable n'a pas de processus pour mettre à l'essai les changements dans un environnement qui simule la configuration de référence avant de mettre en œuvre un changement par rapport à la configuration de référence. (1.5.1)</p> <p>OU</p> |

| Ex. | Niveaux de gravité de la non-conformité | | | |
|------------|---|---|---|--|
| | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | | <p>L'entité responsable n'a pas de processus pour documenter les résultats de l'essai et, si un environnement d'essai a été utilisé, pour documenter les différences entre les environnements d'essai et de production. (1.5.2)</p> <p>OU</p> <p>L'entité responsable n'a pas de processus conforme à l'alinéa 1.6 ni pour vérifier l'identité de la source du logiciel, ni pour vérifier l'intégrité du logiciel obtenu de la source du logiciel, alors que les méthodes appropriées sont mises à la disposition de l'entité responsable par la source du logiciel. (1.6)</p> |
| E2. | Sans objet | Sans objet | Sans objet | <p>L'entité responsable n'a pas documenté ou mis en œuvre de processus pour vérifier, au moins une fois tous les 35 jours civils, s'il y a eu des changements non autorisés à la configuration de référence, pour documenter ceux-ci et pour faire enquête. (2.1)</p> |
| E3. | L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, | L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, | L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, | L'entité responsable n'a mis en œuvre aucun processus d'analyse de vulnérabilité pour un de ses |

| Ex. | Niveaux de gravité de la non-conformité | | | |
|-----|---|---|---|---|
| | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | <p>mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 15 mois et de moins de 18 mois suivant la dernière analyse de l'un de ses <i>systèmes électroniques BES</i> visés. (3.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 36 mois et de moins de 39 mois suivant la dernière analyse active de l'un de ses <i>systèmes électroniques BES</i> visés. (3.2)</p> | <p>mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 18 mois et de moins de 21 mois suivant la dernière analyse de l'un de ses <i>systèmes électroniques BES</i> visés. (3.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 39 mois et de moins de 42 mois suivant la dernière analyse active de l'un de ses <i>systèmes électroniques BES</i> visés. (3.2)</p> | <p>mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 21 mois et de moins de 24 mois suivant la dernière analyse de l'un de ses <i>systèmes électroniques BES</i> visés. (3.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 42 mois et de moins de 45 mois suivant la dernière analyse active de l'un de ses <i>systèmes électroniques BES</i> visés. (3.2)</p> | <p><i>systèmes électroniques BES</i> visés. (E3)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, mais elle a effectué une analyse de vulnérabilité plus de 24 mois suivant la dernière analyse de l'un de ses <i>systèmes électroniques BES</i> visés. (3.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 45 mois suivant la dernière analyse active de l'un de ses <i>systèmes électroniques BES</i> visés. (3.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre et documenté un ou plusieurs processus d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, mais elle n'a pas effectué l'analyse</p> |

| Ex. | Niveaux de gravité de la non-conformité | | | |
|------------|--|--|--|---|
| | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | | <p>de vulnérabilité active d'une manière qui simule une configuration de référence existante de ses <i>systèmes électroniques BES</i> visés. (3.3)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses <i>systèmes électroniques BES</i> visés, mais elle n'a pas documenté les résultats des analyses de vulnérabilité, les plans d'action pour corriger ou atténuer les vulnérabilités constatées dans les analyses, la date planifiée d'achèvement du plan d'action et l'état d'exécution des plans d'atténuation. (3.4)</p> |
| E4. | <p>L'entité responsable a documenté son ou ses plans concernant les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas géré ses <i>actifs électroniques temporaires</i> conformément à la section 1.1 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)</p> <p>OU</p> | <p>L'entité responsable a documenté son ou ses plans concernant les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas mis en œuvre les mesures applicables aux <i>supports de stockage amovibles</i> conformément à la section 3 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)</p> | <p>L'entité responsable a documenté son ou ses plans concernant les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas établi les autorisations relatives aux <i>actifs électroniques temporaires</i> conformément à la section 1.2 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)</p> <p>OU</p> | <p>L'entité responsable n'a pas documenté ou mis en œuvre un ou plusieurs plans concernant les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i> conformément à l'exigence E4 de la norme CIP-010-3. (E4)</p> |

| Ex. | Niveaux de gravité de la non-conformité | | | |
|-----|--|--|---|--------------|
| | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | <p>L'entité responsable a documenté son ou ses plans concernant les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas documenté les mesures applicables aux <i>supports de stockage amovibles</i> conformément à la section 3 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)</p> <p>OU</p> <p>L'entité responsable a documenté son ou ses plans concernant les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas documenté les autorisations relatives aux <i>actifs électroniques temporaires</i> qu'elle gère elle-même conformément à la section 1.2 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)</p> | <p>OU</p> <p>L'entité responsable a documenté son ou ses plans concernant les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas documenté les mesures d'atténuation du risque lié aux vulnérabilités logicielles, à l'introduction de programmes malveillants ou aux utilisations non autorisées pour des <i>actifs électroniques temporaires</i> gérés par l'entité responsable conformément aux sections 1.3, 1.4 et 1.5 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)</p> <p>OU</p> <p>L'entité responsable a documenté son ou ses plans concernant les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas documenté les mesures d'atténuation du risque lié aux vulnérabilités logicielles ou à l'introduction de programmes malveillants pour des <i>actifs électroniques temporaires</i> gérés par une tierce partie conformément aux sections 2.1, 2.2 et 2.3 de l'annexe 1</p> | <p>L'entité responsable a documenté son ou ses plans concernant les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas mis en œuvre les mesures d'atténuation du risque lié aux vulnérabilités logicielles, à l'introduction de programmes malveillants ou aux utilisations non autorisées pour des <i>actifs électroniques temporaires</i> gérés par l'entité responsable conformément aux sections 1.3, 1.4 et 1.5 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)</p> <p>OU</p> <p>L'entité responsable a documenté son ou ses plans concernant les <i>actifs électroniques temporaires</i> et les <i>supports de stockage amovibles</i>, mais n'a pas mis en œuvre les mesures d'atténuation du risque lié aux vulnérabilités logicielles ou à l'introduction de programmes malveillants pour des <i>actifs électroniques temporaires</i> gérés par une tierce partie conformément aux sections 2.1, 2.2 et 2.3 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-3. (E4)</p> | |

| Ex. | Niveaux de gravité de la non-conformité | | | |
|-----|---|--|-----------|--------------|
| | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | complémentaire à l'exigence E4 de la norme CIP-010-3. (E4) | | |

D. Différences régionales

Aucune.

E. Documents connexes

- Plan de mise en œuvre du projet 2019-03.
- Justification technique de la norme CIP-010-4.

Historique des versions

| Version | Date | Intervention | Suivi des modifications |
|---------|------------------|---|--|
| 1 | 26 novembre 2012 | Adoption par le Conseil d'administration de la NERC. | Cette norme encadre la gestion des changements de configuration et des analyses de vulnérabilité en coordination avec d'autres normes CIP et met en œuvre certaines dispositions de l'ordonnance 706 de la FERC. |
| 1 | 22 novembre 2013 | Ordonnance de la FERC approuvant la norme CIP-010-1. (L'ordonnance entre en vigueur le 3 février 2014.) | |
| 2 | 13 novembre 2014 | Adoption par le Conseil d'administration de la NERC. | Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication. |
| 2 | 12 février 2015 | Adoption par le Conseil d'administration de la NERC. | Remplace la version adoptée par le Conseil le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de |

| | | | |
|---|------------------------------|--|--|
| | | | l'ordonnance 791 relativement aux actifs temporaires et aux <i>systèmes électroniques BES</i> à impact faible. |
| 2 | 21 janvier 2016 | Ordonnance de la FERC approuvant la norme CIP-010-3. Dossier RM15-14-000. | |
| 3 | 20 juillet 2017 | Modifications visant à répondre à certaines directives de l'Ordonnance 829 de la FERC. | Révision |
| 3 | 10 août 2017 | Adoption par le Conseil d'administration de la NERC. | |
| 3 | 18 octobre 2018 | Ordonnance de la FERC approuvant la norme CIP-010-3. Dossier RM17-13-000. | |
| 4 | 1er août 2019 | Modifications visant à répondre à certaines prescriptions de l'Ordonnance 850 de la FERC. | Révision |
| 4 | 5 novembre 2020 | Adoption par le Conseil d'administration de la NERC. | |
| 4 | 18 mars 2021 | Lettre d'ordonnance RD21-2-000 de la FERC approuvant la <i>norme de fiabilité</i> CIP-010-4. | |
| 4 | 1 ^{er} octobre 2022 | Date d'entrée en vigueur. | |

CIP-010-4 – Annexe 1

Exigences détaillées des plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*

Les entités responsables doivent intégrer chacune des sections suivantes à leurs plans, prescrits à l'exigence E4, concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*.

Section 1. *Actifs électroniques temporaires* gérés par l'entité responsable.

- 1.1. Gestion des *actifs électroniques temporaires* : Les entités responsables doivent gérer leurs *actifs électroniques temporaires*, individuellement ou par groupe : 1) en permanence, afin d'assurer la conformité avec les exigences pertinentes en tout temps ; 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.
- 1.2. Autorisations relatives aux *actifs électroniques temporaires* : Pour chaque *actif électronique temporaire* ou groupe d'*actifs électroniques temporaires*, chaque entité responsable doit autoriser :
 - 1.1.1. les utilisateurs (individuellement, par groupe ou par rôle) ;
 - 1.1.2. les emplacements (individuellement ou par groupe) ; et
 - 1.1.3. les utilisations, qui doivent être limitées aux actions nécessaires pour assurer les fonctions opérationnelles.
- 1.3. Atténuation du risque lié aux vulnérabilités logicielles : Utiliser 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 les capacités 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.
- 1.4. Atténuation du risque lié à l'introduction de programmes malveillants : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants (selon les capacités de l'*actif électronique temporaire*) :
 - logiciel antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code ;
 - liste blanche d'applications ; ou
 - autres moyens d'atténuer le risque lié à l'introduction de programmes malveillants.

1.5. Atténuation du risque lié aux utilisations non autorisées : Utiliser 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. *Actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable.

2.1. Atténuation du risque lié aux vulnérabilités logicielles : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié aux vulnérabilités présentées par les logiciels sans correctifs dans l'*actif électronique temporaire* (selon les capacités 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.

2.2. Atténuation du risque lié à l'introduction de programmes malveillants : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants (selon les capacités de l'*actif électronique temporaire*) :

- 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'atténuation du risque lié aux programmes malveillants.

2.3. 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, l'entité responsable doit déterminer si d'autres mesures d'atténuation sont nécessaires et appliquer ces mesures avant de connecter l'*actif électronique temporaire*.

Section 3. *Supports de stockage amovibles*

3.1. Autorisations relatives aux supports de stockage amovibles : Pour chaque *support de stockage amovible* ou groupe de *supports de stockage amovibles*, chaque entité responsable doit autoriser :

- 3.1.1.** les utilisateurs (individuellement, par groupe ou par rôle) ; et

- 3.1.2.** les emplacements (individuellement ou par groupe).
- 3.2.** Atténuation du risque lié aux programmes malveillants : Afin de 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, chaque entité responsable doit :
 - 3.2.1.** 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
 - 3.2.2.** 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.

CIP-010-4 – Annexe 2

Exemples de pièces justificatives pour les plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*

- Section 1.1 : Exemples non limitatifs de pièces justificatives pour la section 1.1 : méthodes de gestion des *actifs électroniques temporaires*. Cette information peut faire partie des plans concernant les *actifs électroniques temporaires*, de la documentation concernant les autorisations relatives aux *actifs électroniques temporaires* gérés par l'entité responsable, ou encore d'une politique de sécurité.
- Section 1.2 : Exemples non limitatifs de pièces justificatives pour la section 1.2 : documentation de systèmes de gestion des actifs ou de gestion des ressources humaines, ou formulaires ou feuilles de chiffrier indiquant les autorisations relatives aux *actifs électroniques temporaires* gérés par l'entité responsable. Cette information peut aussi être documentée dans le document principal du plan.
- Section 1.3 : Exemples non limitatifs de pièces justificatives pour la section 1.3 : documentation des moyens utilisés pour atténuer le risque lié aux vulnérabilités présentées par les logiciels sans correctifs, comme la gestion des correctifs de sécurité, l'utilisation de systèmes d'exploitation sur support non inscriptible, le renforcement du système d'exploitation ou d'autres moyens d'atténuation appropriés. Les pièces justificatives peuvent provenir de systèmes de gestion des changements, de solutions de gestion systématique des correctifs, de procédures ou processus concernant l'utilisation de systèmes d'exploitation sur support amovible, ou de procédures ou processus associés aux pratiques de renforcement du système d'exploitation. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié aux vulnérabilités présentées par les logiciels sans correctifs, les pièces justificatives peuvent comprendre une documentation du fournisseur ou de l'entité responsable indiquant que l'*actif électronique temporaire* n'a pas cette capacité.
- Section 1.4 : Exemples non limitatifs de pièces justificatives pour la section 1.4 : documentation des moyens utilisés pour atténuer le risque lié à l'introduction de programmes malveillants, comme des logiciels antivirus et des processus de gestion des mises à jour des signatures ou des séquences de code, des pratiques de liste blanche d'applications, des processus de restriction des communications ou d'autres moyens d'atténuation appropriés. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation du fournisseur ou de l'entité responsable indiquant que l'*actif électronique temporaire* n'a pas cette capacité.
- Section 1.5 : Exemples non limitatifs de pièces justificatives pour la section 1.5 : documentation (politiques ou procédures) des moyens de restriction des accès physiques ; description de la solution de cryptage de disque intégral et du protocole d'authentification ; description de la solution d'authentification multifactorielle ; ou documentation d'autres moyens d'atténuer le risque lié aux utilisations non autorisées.
- Section 2.1 : Exemples non limitatifs de pièces justificatives pour la section 2.1 : documentation de systèmes de gestion des changements, courriels ou procédures qui documentent un examen des correctifs de sécurité installées ; notes de service, courriels, politiques ou contrats d'une tierce partie autre que l'entité responsable qui décrivent le processus

d'application de correctifs ou d'atténuation du risque lié aux vulnérabilités exécuté par la tierce partie ; pièces justificatives de systèmes de gestion des changements, courriels, documentation de système ou contrats indiquant que l'entité responsable juge acceptables les pratiques de la tierce partie ; ou documentation d'autres moyens d'atténuation du risque lié aux vulnérabilités logicielles d'*actifs électroniques temporaires* gérés par la tierce partie. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié aux vulnérabilités présentées par les logiciels sans correctifs, les pièces justificatives peuvent comprendre une documentation de l'entité responsable ou de la tierce partie indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Section 2.2 : Exemples non limitatifs de pièces justificatives pour la section 2.2 : documentation de systèmes de gestion des changements, courriels ou procédures qui documentent un examen du degré de maintien à jour des antivirus installés ; notes de service, courriels, documentation de système, politiques ou contrats d'une tierce partie autre que l'entité responsable qui décrivent le processus de mise à jour des antivirus, l'utilisation d'une liste blanche d'applications, l'utilisation de systèmes d'exploitation sur support externe ou le renforcement du système d'exploitation par la tierce partie ; pièces justificatives de systèmes de gestion des changements, courriels ou contrats indiquant que l'entité responsable juge acceptables les pratiques de la tierce partie ; ou documentation d'autres moyens d'atténuation du risque lié à l'introduction de programmes malveillants pour les *actifs électroniques temporaires* gérés par la tierce partie. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation de l'entité responsable ou de la tierce partie indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Section 2.3 : Exemples non limitatifs de pièces justificatives pour la section 2.3 : documentation de systèmes de gestion des changements, courriels ou contrats attestant qu'un examen a été effectué pour déterminer le besoin de mesures d'atténuation supplémentaires, et que ces mesures ont été mises en œuvre avant la connexion de l'*actif électronique temporaire* géré par une tierce partie autre que l'entité responsable.

Section 3.1 : Exemples non limitatifs de pièces justificatives pour la section 3.1 : documentation de systèmes de gestion des actifs ou de gestion des ressources humaines, formulaires ou feuilles de chiffrier indiquant les autorisations relatives aux *supports de stockage amovibles*. La documentation doit désigner les *supports de stockage amovibles* (individuellement ou par groupe), les utilisateurs autorisés (individuellement, par groupe ou par rôle) et les emplacements autorisés (individuellement ou par groupe).

Section 3.2 : Exemples non limitatifs de pièces justificatives pour la section 3.2 : processus documentés des moyens d'atténuation du risque lié aux programmes malveillants, comme les résultats de balayage paramétré pour les *supports de stockage amovibles* ou la mise en œuvre du balayage à la demande ; processus documentés des moyens d'atténuation du risque lié aux programmes malveillants détectés sur les *supports de stockage amovibles*, comme les journaux créés par les mécanismes de détection qui montrent les résultats du balayage et indiquent la neutralisation des programmes malveillants détectés sur les *supports de stockage amovibles*, ou une confirmation documentée par l'entité que les *supports de stockage amovibles* sont considérés comme exempts de tout programme malveillant.

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme CIP-010-4 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

La présente annexe établit les dispositions particulières d'application au Québec de la norme qu'elle vise. Les dispositions de la norme visée et de l'annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe a préséance.

A. Introduction

1. **Titre :** Aucune disposition particulière.
2. **Numéro :** Aucune disposition particulière.
3. **Objet :** Aucune disposition particulière.

4. **Applicabilité :**

- 4.1. **Entités fonctionnelles**

Aucune disposition particulière.

- 4.2. **Installations**

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

- Toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'installation est de 300 MVA ou moins et (2) aucun groupe de l'installation ne peut être synchronisé avec un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur :**

- 5.1. Adoption de la norme par la Régie de l'énergie : 11 février 2022
 - 5.2. Adoption de l'annexe par la Régie de l'énergie : 11 février 2022
 - 5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : 1^{er} octobre 2023

6. **Contexte :** Aucune disposition particulière.

B. Exigences et mesures

Pour l'exigence E3 et la mesure M3, remplacer toute référence à la *norme de fiabilité* CIP-010-3 par la *norme de fiabilité* CIP-010-4.

C. Conformité

1. **Processus de surveillance de la conformité**

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme CIP-010-4 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

1.1. Responsable des mesures pour assurer la conformité

Au Québec, le terme *responsable des mesures pour assurer la conformité* désigne la Régie de l'énergie dans le rôle visant à surveiller la conformité avec la *norme de fiabilité* visée et à la présente annexe, et à assurer l'application de celles-ci.

1.2. Conservation des pièces justificatives

Aucune disposition particulière.

1.3. Programme de surveillance de la conformité et d'application des normes

La Régie de l'énergie établit les processus de surveillance qui servent à évaluer les données ou l'information afin de déterminer la conformité ou la non-conformité avec la *norme de fiabilité* visée et avec la présente annexe.

Niveaux de gravité de la non-conformité (VSL)

Pour tous les niveaux de gravité de la non-conformité de l'exigence E4, remplacer toute référence à la *norme de fiabilité* CIP-010-3 par la *norme de fiabilité* CIP-010-4.

D. Différences régionales

Aucune disposition particulière.

E. Documents connexes

Aucune disposition particulière.

CIP-010-4 – Annexe 1

Aucune disposition particulière.

CIP-010-4 – Annexe 2

Aucune disposition particulière.

Historique des versions

| Version | Date | Intervention | Suivi des modifications |
|---------|-----------------|---|-------------------------|
| 1 | 11 février 2022 | Nouvelle annexe en suivi de la décision D-2022-021. | Nouvelle |