

## A. Introduction

1. **Titre :** Cybersécurité — Personnel et formation
2. **Numéro :** CIP-004-6
3. **Objet :** Réduire au minimum les risques de compromissions susceptibles d'entraîner un fonctionnement incorrect ou une instabilité du *système de production-transport d'électricité (BES)* et attribuables à des personnes qui accèdent à des *systèmes électroniques BES*, en exigeant une évaluation des risques liés au personnel, une formation et une sensibilisation à la sécurité qui soient adéquates pour protéger ces *systèmes électroniques BES*.
4. **Applicabilité :**
  - 4.1. **Entités fonctionnelles :** Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier 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 *installations*, systèmes, et équipements suivants pour la protection ou la remise en charge du *BES* :
      - 4.1.2.1. Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge 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 du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant.
      - 4.1.2.2. Chaque *automatisme de réseau* (SPS) ou *plan de défense* (RAS) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.
      - 4.1.2.3. Chaque *système de protection* applicable au *transport* (à l'exclusion des systèmes DSF et DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.
      - 4.1.2.4. Chaque *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 des échanges ou responsable des échanges**

**4.1.6. Coordonnateur de la fiabilité**

**4.1.7. Exploitant de réseau de transport**

**4.1.8. Propriétaire d'installation de transport**

**4.2. Installations :** Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

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

**4.2.1.1.** Chaque 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 du délestage automatique de *charge* de 300 MW ou plus un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant.

**4.2.1.2.** Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

**4.2.1.3.** Chaque *système de protection* applicable au *transport* (à l'exclusion des DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

**4.2.1.4.** Chaque *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-004-6 :

- 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 électroniques* 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 déterminent qu'elles n'ont pas de systèmes électroniques BES catégorisés comme « impact élevé » ou « impact moyen » en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

**5. Dates d'entrée en vigueur :**

Voir le plan de mise en œuvre de la norme CIP-004-6.

**6. Contexte :**

La norme CIP-004 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi 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 DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *BES*. Un examen des tolérances des systèmes 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 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. La SDT (équipe de rédaction) 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 », conformément au processus d'identification et de catégorisation de la norme CIP-002-5.1.

- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », processus de désignation et de catégorisation de la norme CIP-002-5.1.
- **Systèmes électroniques BES à impact moyen à connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à *connectivité externe routable*, à l'exclusion des *actifs électroniques* des *systèmes électroniques BES* auxquels on ne peut avoir accès directement par *connectivité externe routable*.
- **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* associé à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.

## 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-004-6) – Programme de sensibilisation à la sécurité.  
*[Facteur de risque de non-conformité : faible] [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-004-6) – Programme de sensibilisation à la sécurité ; ainsi que des pièces justificatives additionnelles pour démontrer la mise en œuvre tel que décrit dans la colonne Mesures du tableau.

Tableau E1 (CIP-004-6) – Programme de sensibilisation à la sécurité			
Alinéa	Systèmes visés	Exigences	Mesures
1.1	<p><i>Systèmes électroniques BES à impact élevé.</i></p> <p><i>Systèmes électroniques BES à impact moyen.</i></p>	<p>Une sensibilisation à la sécurité qui, au moins une fois par trimestre civil, rappelle les pratiques de cybersécurité (pouvant inclure les pratiques de sécurité physique associées) au personnel de l'entité responsable qui a un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des <i>systèmes électroniques BES</i>.</p>	<p>Exemple non limitatif de pièces justificatives : des documents attestant que le rappel trimestriel a été fait.</p> <p>Exemples non limitatifs de pièces justificatives du rappel : des copies datées de l'information utilisée pour rappeler les pratiques de sécurité et des preuves de distribution, notamment :</p> <ul style="list-style-type: none"> <li>• communications ciblées (p. ex., courriels, notes de service, formation en ligne, etc.) ;</li> <li>• communications générales (p. ex., affiches, intranet, brochures, etc.) ; ou</li> <li>• rappels et soutien de la direction (p. ex., présentations, réunions, etc.).</li> </ul>

- E2.** Chaque entité responsable doit mettre en œuvre un ou des programmes de formation sur la cybersécurité axée sur les rôles, les fonctions ou les responsabilités de chacun, qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité.

*[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]*

- M2.** Les pièces justificatives doivent comprendre les programmes de formation qui couvrent tous les alinéas applicables du tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité ; d'autres pièces justificatives doivent attester la mise en œuvre des programmes.

Tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité			
Alinéa	Systèmes visés	Exigences	Mesures
2.1	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	<p>Formation portant sur :</p> <ol style="list-style-type: none"> <li>2.1.1. les politiques de cybersécurité ;</li> <li>2.1.2. le contrôle des accès physiques ;</li> <li>2.1.3. le contrôle des accès électroniques ;</li> <li>2.1.4. le programme de contrôle des visiteurs ;</li> <li>2.1.5. la gestion et le stockage de l'information des <i>systèmes électroniques BES</i> ;</li> <li>2.1.6. la détection des <i>incidents de cybersécurité</i> et l'envoi des avis initiaux conformément au plan d'intervention en cas d'incident de l'entité ;</li> <li>2.1.7. les plans de rétablissement des <i>systèmes électroniques BES</i> ;</li> <li>2.1.8. l'intervention en cas d'<i>incident de cybersécurité</i> ; et</li> <li>2.1.9. les risques pour la cybersécurité</li> </ol>	<p>Exemples non limitatifs de pièces justificatives : matériel de formation comme des présentations PowerPoint, des notes à l'intention des formateurs ou des étudiants, ou des documents de cours.</p>

Tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité			
Alinéa	Systèmes visés	Exigences	Mesures
		associés à l'interconnectabilité et à l'interopérabilité des <i>systèmes électroniques BES</i> avec d'autres <i>actifs électroniques</i> , y compris des <i>actifs électroniques transitoires</i> et des <i>supports de stockage amovibles</i> .	
2.2	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES</i> à impact moyen à <i>connectivité externe routable</i> et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	Exiger que soit suivie au complet la formation énoncée à l'alinéa 2.1 avant que soit accordé un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des <i>actifs électroniques</i> visés, sauf dans des <i>circonstances CIP exceptionnelles</i> .	Exemples non limitatifs de pièces justificatives : registres de formation et documents attestant l'invocation de <i>circonstances CIP exceptionnelles</i> .
2.3	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES</i> à impact moyen à <i>connectivité externe routable</i> et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	Exiger que la formation énoncée à l'alinéa 2.1 soit suivie au complet au moins une fois tous les 15 mois civils.	Exemple non limitatif de pièces justificatives : registres de formation individuels datés.

- E3.** Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés d'évaluation des risques liés au personnel en vue de l'octroi ou du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement à des *systèmes électroniques BES* et qui, collectivement, couvrent tous les parties alinéas applicables du tableau E3 (CIP-004-6) – Programme d'évaluation des risques liés au personnel.

*[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]*

- M3.** Les pièces justificatives doivent comprendre le ou les programmes documentés d'évaluation des risques liés au personnel qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-004-6) – Programme d'évaluation des risques liés au personnel ; d'autres pièces justificatives doivent attester la mise en œuvre du ou des programmes.

Tableau E3 (CIP-004-6) – Programme d'évaluation des risques liés au personnel			
Alinéa	Systèmes visés	Exigences	Mesures
3.1	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES</i> à impact moyen à <i>connectivité externe routable</i> et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	Processus de confirmation de l'identité.	Exemple non limitatif de pièces justificatives : documents attestant le processus suivi par l'entité responsable pour confirmer l'identité.

Tableau E3 (CIP-004-6) – Programme d'évaluation des risques liés au personnel			
Alinéa	Systèmes visés	Exigences	Mesures
3.2	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	<p>Processus de vérification des antécédents judiciaires sur les sept années précédentes dans le cadre de chaque évaluation des risques liés au personnel, qui comprend :</p> <p>3.2.1. le lieu où réside actuellement la personne, peu importe depuis combien de temps ; et</p> <p>3.2.2. les autres endroits où, au cours des sept années précédant la date de vérification des antécédents judiciaires, la personne a résidé pendant au moins six mois consécutifs.</p> <p>S'il est impossible de mener une vérification complète des antécédents judiciaires sur les sept années précédentes, pousser la vérification le plus loin possible et consigner les motifs pour lesquels la vérification complète sur cette période n'a pu se faire.</p>	<p>Exemple non limitatif de pièces justificatives : documents attestant le processus suivi par l'entité responsable pour vérifier les antécédents criminels sur les sept dernières années.</p>

Tableau E3 (CIP-004-6) – Programme d'évaluation des risques liés au personnel			
Alinéa	Systèmes visés	Exigences	Mesures
3.3	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	Critères ou processus pour évaluer les résultats de la vérification des antécédents judiciaires en vue d'autoriser un accès.	Exemple non limitatif de pièces justificatives : documents attestant le processus de l'entité responsable pour évaluer les résultats des vérifications des antécédents judiciaires.
3.4	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	Critères ou processus pour vérifier que les évaluations des risques liés au personnel dont les contractuels et les fournisseurs de services doivent faire l'objet sont menées conformément aux alinéas 3.1 à 3.3.	Exemples non limitatifs de pièces justificatives : documents attestant les critères ou le processus de l'entité responsable pour vérifier les évaluations des risques liés au personnel pour les contractuels et les fournisseurs de services.
3.5	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	Processus permettant de s'assurer que les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement ont fait l'objet d'une évaluation des risques liés au personnel conformément aux alinéas 3.1 à 3.4 au cours des sept dernières années.	Exemples non limitatifs de pièces justificatives : documents attestant le processus suivi par l'entité responsable pour s'assurer que les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement ont fait l'objet d'une évaluation des risques liés au personnel au cours des sept dernières années.

- E4.** Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de gestion des accès qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-004-6) – Programme de gestion des accès.

*[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation le même jour]*

- M4.** Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-004-6) – Programme de gestion des accès ; d'autres pièces justificatives doivent attester la mise en œuvre des mesures du programme de gestion des accès selon la colonne Mesures du tableau.

Tableau E4 (CIP-004-6) – Programme de gestion des accès			
Alinéa	Systèmes visés	Exigences	Mesures
4.1	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	<p>Processus d'autorisation selon le besoin déterminé par l'entité responsable, sauf dans des <i>circonstances CIP exceptionnelles</i> :</p> <ol style="list-style-type: none"> <li>4.1.1. de l'accès électronique ;</li> <li>4.1.2. de l'accès physique sans accompagnement dans un <i>périmètre de sécurité physique</i> ; et</li> <li>4.1.3. de l'accès à des emplacements de stockage (physiques ou électroniques) désignés pour l'information de <i>système électronique BES</i>.</li> </ol>	<p>Exemples non limitatifs de pièces justificatives : documents datés attestant le processus suivi pour autoriser un accès électronique, un accès physique sans accompagnement à un <i>périmètre de sécurité physique</i> et un accès à des emplacements de stockage (physiques ou électroniques) désignés pour l'information de <i>système électronique BES</i>.</p>

Tableau E4 (CIP-004-6) – Programme de gestion des accès

Alinéa	Systèmes visés	Exigences	Mesures
4.2	<p><i>Systèmes électroniques BES à impact élevé</i> et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable</i> et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	Vérifier, au moins une fois par trimestre civil, que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d'accès autorisé.	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> <li>• documents datés attestant une comparaison entre la liste automatisée des personnes pour lesquelles on a autorisé l'accès (base de données des activités de fourniture) et la liste automatisée des personnes auxquelles on a fourni un accès (liste des comptes utilisateurs) ; ou</li> <li>• documents datés attestant une comparaison entre la liste des personnes pour lesquelles on a autorisé l'accès (formulaires d'autorisation) et la liste des personnes auxquelles on a fourni un accès (formulaires de fourniture d'accès ou liste des comptes partagés).</li> </ul>

Tableau E4 (CIP-004-6) – Programme de gestion des accès

Alinéa	Systèmes visés	Exigences	Mesures
4.3	<p><i>Systèmes électroniques BES à impact élevé</i> et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable</i> et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	<p>Dans le cas des accès électroniques, vérifier, au moins une fois tous les 15 mois civils, que tous les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont correctement attribués et qu'ils sont ceux jugés nécessaires par l'entité responsable.</p>	<p>Exemples non limitatifs de pièces justificatives : documentation de l'examen, y compris tous les éléments suivants :</p> <ol style="list-style-type: none"> <li>1. liste datée de tous les comptes ou groupes de comptes ou rôles au sein du système ;</li> <li>2. description sommaire des droits d'accès associés à chaque groupe ou rôle ;</li> <li>3. comptes attribués au groupe ou au rôle ; et</li> <li>4. preuve datée attestant qu'on a vérifié que les droits d'accès du groupe sont autorisés et qu'ils correspondent aux fonctions de toute personne à qui ils sont attribués.</li> </ol>

Tableau E4 (CIP-004-6) – Programme de gestion des accès

Alinéa	Systèmes visés	Exigences	Mesures
4.4	<p><i>Systèmes électroniques BES à impact élevé</i> et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable</i> et :</p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	Vérifier, au moins une fois tous les 15 mois civils, que les accès aux emplacements de stockage (physiques ou électroniques) désignés pour l'information de <i>système électronique BES</i> sont correctement attribués et qu'ils correspondent à ce que l'entité responsable juge nécessaire pour les tâches à accomplir.	<p>Exemples non limitatifs de pièces justificatives : documentation de l'examen, y compris tous les éléments suivants :</p> <ol style="list-style-type: none"> <li>1. liste datée des autorisations d'accès à l'information de <i>système électronique BES</i> ;</li> <li>2. droits d'accès associés aux autorisations ; et</li> <li>3. preuve datée attestant qu'on s'est assuré que les autorisations et les droits d'accès sont correctement attribués et qu'ils correspondent au minimum nécessaire pour les tâches à accomplir.</li> </ol>

- E5.** Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de révocation d'accès qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-004-6) – Révocation d'accès.

*[Facteur de risque de non-conformité : moyen] [Horizon : exploitation le même jour et planification de l'exploitation]*

- M5.** Les pièces justificatives doivent comprendre chacun des programmes documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-004-6) – Révocation d'accès ; d'autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

Tableau E5 (CIP-004-6) – Révocation d'accès			
Alinéa	Systèmes visés	Exigences	Mesures
5.1	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> <li>1. les <i>EACMS</i> associés ; et</li> <li>2. les <i>PACS</i> associés.</li> </ol>	<p>Processus déclenchant le retrait à une personne de la possibilité d'accès physique sans accompagnement et d'<i>accès distant interactif</i> lors de son départ et menant à bien ce processus dans un délai de 24 heures suivant le départ. (Le retrait de la possibilité d'accès peut différer de la suppression, de la désactivation, de la révocation ou du retrait de tous les droits d'accès.)</p>	<p>Exemples non limitatifs de pièces justificatives :</p> <ol style="list-style-type: none"> <li>1. formulaire d'activité ou d'approbation daté qui confirme le retrait d'accès associé au départ ; et</li> <li>2. journaux ou autres preuves attestant que la personne ne dispose plus d'un accès.</li> </ol>

Tableau E5 (CIP-004-6) – Révocation d'accès			
Alinéa	Systèmes visés	Exigences	Mesures
5.2	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> <li>1. les EACMS associés ; et</li> <li>2. les PACS associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> <li>3. les EACMS associés ; et</li> <li>4. les PACS associés.</li> </ol>	Dans le cas d'une réaffectation ou d'une mutation, révoquer l'accès électronique autorisé aux comptes individuels et l'accès physique sans accompagnement autorisé que l'entité responsable juge non nécessaires avant la fin du jour civil suivant la date, déterminée par l'entité responsable, où la personne n'a plus besoin de ces accès.	<p>Exemples non limitatifs de pièces justificatives :</p> <ol style="list-style-type: none"> <li>1. formulaire d'activité ou d'approbation daté attestant l'examen des accès logique et physique ; et</li> <li>2. journaux ou autres preuves attestant que la personne ne dispose plus des accès que l'entité responsable détermine comme n'étant plus nécessaires.</li> </ol>
5.3	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> <li>1. les EACMS associés ; et</li> <li>2. les PACS associés.</li> </ol> <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> <li>1. les EACMS associés ; et</li> <li>2. les PACS associés.</li> </ol>	Dans le cas d'un départ, révoquer l'accès de la personne aux emplacements de stockage désignés pour l'information de <i>système électronique BES</i> , qu'ils soient physiques ou électroniques (à moins que l'accès ait déjà été révoqué selon l'exigence E5.1), avant la fin du jour civil suivant la date à laquelle prend effet le départ.	Exemple non limitatif de pièce justificative : formulaire d'activité ou d'approbation attestant le retrait de l'accès aux emplacements physiques ou aux systèmes électroniques désignés pour l'information de <i>système électronique BES</i> daté au plus tard du jour civil suivant le départ.

Tableau E5 (CIP-004-6) – Révocation d'accès			
Alinéa	Systèmes visés	Exigences	Mesures
5.4	<i>Systèmes électroniques BES</i> à impact élevé et : <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés.</li> </ul>	Dans le cas d'un départ, révoquer l'accès aux comptes utilisateurs non partagés de la personne (à moins que l'accès ait déjà été révoqué selon l'exigence E5.1 ou E5.3) dans les 30 jours civils suivant la date à laquelle prend effet le départ.	Exemple non limitatif de pièce justificative : formulaire d'activité ou d'approbation attestant le retrait de l'accès à un <i>actif électronique BES</i> ou à un logiciel d'application selon ce qui est jugé nécessaire pour mener à bien la révocation d'accès, et daté dans les 30 jours civils suivant le départ.
5.5	<i>Systèmes électroniques BES</i> à impact élevé et : <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés.</li> </ul>	<p>Dans le cas d'un départ, changer les mots de passe des comptes partagés connus de l'utilisateur dans les 30 jours civils suivant le départ. Dans le cas d'une réaffectation ou d'une mutation, changer les mots de passe des comptes partagés connus de l'utilisateur dans les 30 jours civils suivant la date, déterminée par l'entité responsable, où la personne n'a plus besoin de cet accès.</p> <p>Si l'entité responsable détermine et documente qu'un délai plus long est nécessaire en raison de circonstances opérationnelles atténuantes, changer les mots de passe dans les 10 jours civils suivant la fin de ces circonstances.</p>	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> <li>formulaire d'activité ou d'approbation attestant que le mot de passe a été changé dans les 30 jours civils suivant le départ ;</li> <li>formulaire d'activité ou d'approbation attestant que le mot de passe a été changé dans les 30 jours civils suivant la réaffectation ou la mutation ; ou</li> <li>documentation des circonstances opérationnelles atténuantes et formulaire d'activité ou d'approbation attestant que le mot de passe a été changé dans les 10 jours civils suivant la fin de ces circonstances.</li> </ul>

## **C. Conformité**

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

#### **1.1. Responsable des mesures pour assurer la conformité**

Selon la définition des règles de procédure de la NERC, le terme « responsable des mesures pour assurer la conformité » (CEA) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

#### **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 responsable 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 responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable 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 derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

#### **1.3. Processus de surveillance et d'évaluation de la conformité**

Audits de conformité

Déclarations sur la conformité

Contrôles ponctuels

Enquêtes de conformité

Déclarations de non-conformité

Plaintes

#### **1.4. Autres informations sur la conformité**

Aucune

## 2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	Planification de l'exploitation	Faible	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait moins de 10 jours civils après le début d'un trimestre civil subséquent. (1.1)	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait entre 10 et 30 jours civils après le début d'un trimestre civil subséquent. (1.1)	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait au cours du trimestre civil suivant, plus de 30 jours après le début de ce trimestre. (1.1)	L'entité responsable n'a pas documenté ou mis en œuvre un processus de sensibilisation à la sécurité pour rappeler les pratiques de cybersécurité. (E1)  OU  L'entité responsable n'a pas rappelé les pratiques de cybersécurité et les pratiques de sécurité physique associées pendant au moins deux trimestres civils consécutifs. (1.1)
E2	Planification de l'exploitation	Faible	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant un des thèmes de formation des alinéas 2.1.1 à 2.1.9 de	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant deux des thèmes de formation des alinéas 2.1.1 à 2.1.9 de	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant trois des thèmes de formation des alinéas 2.1.1 à 2.1.9 de	L'entité responsable n'a pas mis en œuvre un programme de formation sur la cybersécurité axé sur les rôles, les fonctions ou les responsabilités de

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			l'exigence. (2.1)  OU  L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former une personne (sauf en cas de <i>circonstances CIP exceptionnelles</i> ) avant de lui accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement. (2.2)  OU  L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former une personne ayant un accès électronique autorisé ou un accès physique	l'exigence. (2.1)  OU  L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former deux personnes (sauf en cas de <i>circonstances CIP exceptionnelles</i> ) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement. (2.2)  OU  L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former deux personnes ayant un accès électronique autorisé ou un accès physique	l'exigence. (2.1)  OU  L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former trois personnes (sauf en cas de <i>circonstances CIP exceptionnelles</i> ) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement. (2.2)  OU  L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former trois personnes ayant un accès électronique autorisé ou un accès physique	chacun. (E2)  OU  L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant quatre ou plus des thèmes de formation des alinéas 2.1.1 à 2.1.9 de l'exigence. (2.1)  OU  L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former quatre personnes ou plus (sauf en cas de <i>circonstances CIP exceptionnelles</i> ) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			autorisé sans accompagnement dans les 15 mois civils suivant la fin de la dernière formation qu'elle a suivie. (2.3)	autorisé sans accompagnement dans les 15 mois civils suivant la fin de la dernière formation qu'elle a suivie. (2.3)	autorisé sans accompagnement dans les 15 mois civils suivant la fin de la dernière formation qu'elle a suivie. (2.3)	accompagnement. (2.2)  OU  L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former quatre personnes ou plus ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de fin de la dernière formation qu'elle a suivie. (2.3)
<b>E3</b>	<b>Planification de l'exploitation</b>	<b>Moyen</b>	L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la	L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la	L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la	L'entité responsable n'a pas inclus tous les éléments des alinéas 3.1 à 3.4 dans les programmes documentés d'évaluation des risques liés au personnel (PRA) pour les personnes, y

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p>PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à une personne. (E3)</p> <p>OU</p> <p>L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de service) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité d'une personne. (3.1 et 3.4)</p> <p>OU</p>	<p>PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à deux personnes. (E3)</p> <p>OU</p> <p>L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité de deux personnes. (3.1 et 3.4)</p> <p>OU</p>	<p>PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à trois personnes. (E3)</p> <p>OU</p> <p>L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité de trois personnes. (3.1 et 3.4)</p> <p>OU</p>	<p>compris les contractuels et les fournisseurs de services, en vue de l'obtention et du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement. (E3)</p> <p>OU</p> <p>L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à quatre personnes ou</p>

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p>L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour une personne. (3.2 et 3.4)</p> <p>OU</p> <p>L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services)</p>	<p>L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour deux personnes. (3.2 et 3.4)</p> <p>OU</p> <p>L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services)</p>	<p>L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour trois personnes. (3.2 et 3.4)</p> <p>OU</p> <p>L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services)</p>	<p>plus. (E3)</p> <p>OU</p> <p>L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité de quatre personnes ou plus. (3.1 et 3.4)</p> <p>OU</p> <p>L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour</p>

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p>ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis d'évaluer la vérification des antécédents judiciaires pour l'autorisation d'accès d'une personne. (3.3 et 3.4)</p> <p>OU</p> <p>L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour une personne ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA</p>	<p>ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis d'évaluer la vérification des antécédents judiciaires pour l'autorisation d'accès de deux personnes. (3.3 et 3.4)</p> <p>OU</p> <p>L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour deux personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA</p>	<p>ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis d'évaluer la vérification des antécédents judiciaires pour l'autorisation d'accès de trois personnes. (3.3 et 3.4)</p> <p>OU</p> <p>L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour trois personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA</p>	<p>les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour quatre personnes ou plus. (3.2 et 3.4)</p> <p>OU</p> <p>L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a</p>

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			précédente. (3.5)	précédente. (3.5)	précédente. (3.5)	<p>omis d'évaluer la vérification des antécédents judiciaires pour l'autorisation d'accès de quatre personnes ou plus. (3.3 et 3.4)</p> <p>OU</p> <p>L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour quatre personnes ou plus ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA précédente. (3.5)</p>
<b>E4</b>	<b>Planification de l'exploitation</b>	<b>Moyen</b>	L'entité responsable n'a pas vérifié que les personnes ayant un accès	L'entité responsable n'a pas vérifié que les personnes ayant un accès	L'entité responsable n'a pas vérifié que les personnes ayant un accès	L'entité responsable n'a pas mis en œuvre un programme documenté

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
	<b>et exploitation du jour même</b>		<p>électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d'accès autorisé pendant un trimestre civil, mais l'a fait moins de 10 jours civils après le début d'un trimestre civil subséquent. (4.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires,</p>	<p>électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d'accès autorisé pendant un trimestre civil, mais l'a fait entre 10 et 20 jours civils après le début d'un trimestre civil subséquent. (4.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires,</p>	<p>électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d'accès autorisé pendant un trimestre civil, mais l'a fait entre 20 et 30 jours civils après le début d'un trimestre civil subséquent. (4.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires, ,</p>	<p>pour la gestion des accès. (E4)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs programmes documentés pour la gestion des accès comprenant un processus pour autoriser l'accès électronique, l'accès physique sans accompagnement ou l'accès aux emplacements de stockage désignés pour l'information de <i>système électronique BES</i>. (4.1)</p> <p>OU</p> <p>L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans</p>

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p>mais a constaté que, pour 5 % ou moins de ses <i>systèmes électroniques BES</i>, les droits d'accès étaient incorrects ou non nécessaires. (4.3)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les accès aux emplacements de stockage désignés pour l'information de <i>système électronique BES</i> sont corrects et nécessaires, mais a constaté que pour 5 % ou moins de ses emplacements de stockage de l'information de <i>système électronique BES</i>, les droits d'accès étaient incorrects ou non</p>	<p>mais a constaté que pour plus de 5 % mais au plus 10 % de ses <i>systèmes électroniques BES</i>, les droits d'accès étaient incorrects ou non nécessaires. (4.3)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les accès aux emplacements de stockage désignés pour l'information de <i>système électronique BES</i> sont corrects et nécessaires, mais a constaté que pour plus de 5 % mais au plus 10 % de ses emplacements de stockage de l'information de <i>système électronique</i></p>	<p>mais a constaté que pour plus de 10 % mais au plus 15 % de ses <i>systèmes électroniques BES</i>, les droits d'accès étaient incorrects ou non nécessaires. (4.3)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les accès aux emplacements de stockage désignés pour l'information de <i>système électronique BES</i> sont corrects et nécessaires, mais a constaté que pour plus de 10 % mais au plus 15 % de ses emplacements de stockage de l'information de <i>système électronique</i></p>	<p>accompagnement en vigueur sont consignées dans des registres d'accès autorisé pendant deux trimestres civils consécutifs ou plus. (4.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires, , mais a constaté que pour plus de 15 % de ses <i>systèmes électroniques BES</i>, les droits d'accès étaient incorrects ou non</p>

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			nécessaires. (4.4)	<i>BES</i> , les droits d'accès étaient incorrects ou non nécessaires. (4.4)	<i>BES</i> , les droits d'accès étaient incorrects ou non nécessaires. (4.4)	nécessaires. (4.3)  OU  L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les accès aux emplacements de stockage désignés pour l'information de <i>système électronique BES</i> sont corrects et nécessaires, mais a constaté que pour plus de 15 % de ses emplacements de stockage de l'information de <i>système électronique BES</i> , les droits d'accès étaient incorrects ou non nécessaires. (4.4)
<b>E5</b>	<b>Exploitation du jour même et</b>	<b>Moyen</b>	L'entité responsable a mis en œuvre un ou plusieurs processus pour	L'entité responsable a mis en œuvre un ou plusieurs processus pour	L'entité responsable a mis en œuvre un ou plusieurs processus pour	L'entité responsable n'a mis en œuvre aucun programme documenté

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
	<b>planification de l'exploitation</b>		<p>révoquer l'accès des personnes aux emplacements de stockage désignés pour l'information de <i>système électronique BES</i>, mais dans le cas d'une personne, la révocation n'a pas été faite avant la fin du jour civil suivant la date et l'heure de prise d'effet du départ. (5.3)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès des personnes à leurs comptes utilisateurs lors de leur départ, mais la révocation n'a pas été faite dans les 30 jours civils suivant la date du départ pour une</p>	<p>retirer la capacité d'accès physique sans accompagnement et <i>d'accès distant interactif</i> lors d'un départ ou pour mener à bien ce retrait dans les 24 heures suivant le départ, mais a omis de déclencher ce retrait pour une personne. (5.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer qu'une personne n'a plus besoin de conserver des accès à la suite d'une réaffectation ou d'une mutation, mais, pour une personne, n'a pas révoqué les accès électroniques autorisés aux comptes individuels</p>	<p>retirer la capacité d'accès physique sans accompagnement et <i>d'accès distant interactif</i> lors d'un départ ou pour mener à bien ce retrait dans les 24 heures suivant le départ, mais a omis de déclencher ce retrait pour deux personnes. (5.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer qu'une personne n'a plus besoin de conserver des accès à la suite d'une réaffectation ou d'une mutation, mais, pour deux personnes, n'a pas révoqué les accès électroniques autorisés aux comptes individuels</p>	<p>de révocation d'accès pour les accès électroniques, les accès physiques sans accompagnement ou pour les emplacements de stockage des informations de <i>système électronique BES</i>. (E5)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus pour retirer la capacité d'accès physique sans accompagnement et <i>d'accès distant interactif</i> lors d'un départ ou pour mener à bien ce retrait dans les 24 heures suivant le départ, mais a omis de déclencher ce retrait pour trois personnes ou plus. (5.1)</p>

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			<p>personne ou plus. (5.4)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus pour changer les mots de passe des comptes partagés connus des utilisateurs lors de leur départ, de leur réaffectation ou de leur mutation, mais ce changement n'a pas été fait dans les 30 jours civils suivant la date du départ, de la réaffectation ou de la mutation pour une personne ou plus. (5.5)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer et</p>	<p>et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée. (5.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès des personnes aux emplacements de stockage désignés pour l'information de <i>système électronique BES</i>, mais dans le cas de deux personnes, la révocation n'a pas été faite avant la fin du jour civil suivant la date et l'heure de prise d'effet du départ. (5.3)</p>	<p>et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée. (5.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès des personnes aux emplacements de stockage désignés pour l'information de <i>système électronique BES</i>, mais dans le cas de trois personnes ou plus, la révocation n'a pas été faite avant la fin du jour civil suivant la date et l'heure de prise d'effet du départ. (5.3)</p>	<p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer qu'une personne n'a plus besoin de conserver des accès à la suite d'une réaffectation ou d'une mutation, mais, pour trois personnes ou plus, n'a pas révoqué les accès électroniques autorisés aux comptes individuels et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée. (5.2)</p>

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			documenter les circonstances opérationnelles atténuantes suivant un départ, une réaffectation ou une mutation, mais n'a pas changé un ou plusieurs mots de passe de comptes partagés connus d'un utilisateur dans les 10 jours civils suivant la fin de circonstances opérationnelles atténuantes. (5.5)			

## D. Différences régionales

Aucune.

## E. Interprétations

Aucune.

## F. Documents connexes

Aucun.

## Historique des versions

Version	Date	Modification apportée	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center ».	24 mars 2006
2	30 septembre 2009	<p>Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes.</p> <p>Suppression de la mention sur la prise en compte des considérations d'affaires.</p> <p>Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable.</p> <p>Reformulation de la date d'entrée en vigueur.</p> <p>Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsable de la surveillance de l'application des normes ».</p>	
3	16 décembre 2009	<p>Changement du numéro de version de -2 à -3.</p> <p>Dans l'exigence E1.6, suppression de la phrase concernant le retrait du service d'un composant ou d'un système aux fins d'essais, en réponse à l'ordonnance de la FERC du 30 septembre 2009.</p>	
3	16 décembre 2009	Approbation par le Conseil d'administration de la NERC.	

3	31 mars 2010	Approbation par la FERC.	
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modification en coordination avec les autres normes CIP et révision du format selon le modèle RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-004-5.	
5.1	30 septembre 2013	Modification de deux VSL à l'exigence E4.	Errata
6	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.
6	12 février 2015	Adoption par le conseil d'administration de la NERC.	Remplace la version adoptée par le conseil d'administration 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.

## Principes directeurs et fondements techniques

### Section 4 – Portée de l'applicabilité des normes CIP sur la cybersécurité

La section 4 (Applicabilité) des normes présente de l'information importante pour aider les entités responsables à déterminer la portée d'application des exigences CIP sur la cybersécurité.

La section 4.1 (Entités fonctionnelles) présente la liste des entités fonctionnelles de la NERC auxquelles s'applique la norme. Si l'entité est enregistrée au titre d'une ou de plusieurs des entités fonctionnelles énumérées à la section 4.1, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité à ceux qui détiennent certains types de systèmes et d'équipements énumérés à la section 4.2.

La section 4.2 (Installations) définit la portée des *installations*, systèmes et équipements détenus par l'entité responsable qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. Outre l'ensemble des *installations* du *BES*, des *centres de contrôle* et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements détenus par les *distributeurs*. Bien que le terme « *installations* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela aide à clarifier quels sont les *installations*, systèmes et équipements visés par les normes.

### Exigence E1

Le programme de sensibilisation à la sécurité se veut un programme d'information, et non de formation. Il devrait rappeler les pratiques de sécurité afin de tenir le personnel au courant des pratiques recommandées en matière de sécurité physique et électronique pour protéger les *systèmes électroniques BES*. L'entité responsable n'a pas à fournir des documents qui attestent que chaque personne a reçu ou compris l'information, mais elle doit conserver en tout temps le matériel utilisé pour le programme : affiches, notes de service, présentations, etc.

Voici des exemples de mécanismes ou preuves de sensibilisation qu'on peut utiliser s'ils sont datés :

- communications ciblées (courriels, notes de service, formation en ligne, etc.) ;
- communications générales (affiches, intranet, brochures, etc.) ;
- rappels et soutien de la direction (présentations, réunions, etc.).

### Exigence E2

La formation doit porter sur les politiques, les contrôles d'accès et les procédures établis pour les *systèmes électroniques BES* ; elle doit comporter au moins les éléments nécessaires en fonction des rôles et responsabilités de chacun, selon le tableau E2. L'entité responsable a la liberté de définir son propre programme de formation, qui peut comprendre plusieurs modules et modes de prestation, mais un seul programme de formation pour toutes les personnes à former est aussi acceptable. L'entité responsable peut, à sa guise, axer la formation sur les fonctions, les rôles ou les responsabilités.

Le paragraphe 434 de l'ordonnance 706 de la FERC intègre à la formation un nouvel élément qui concerne les équipements et les logiciels de réseau ainsi que d'autres éléments d'interconnectabilité

électronique nécessaires à l'exploitation et au contrôle des *systèmes électroniques BES*. La formation doit également porter sur les risques associés au branchement et à l'utilisation d'*actifs électroniques transitoires* et de *supports de stockage amovibles* dans des *systèmes électroniques BES* ou à l'intérieur d'un *périmètre de sécurité électronique*. Comme l'indique le paragraphe 135 de l'ordonnance 791 de la FERC, des *actifs électroniques transitoires* et des *supports de stockage amovibles* ont été la cause de cas concrets de contamination de systèmes de commande industrielle de production d'électricité par des maliciels ; la formation à leur utilisation est donc essentielle pour la protection des *systèmes électroniques BES*. Il ne s'agit pas de donner une formation technique aux personnes responsables des équipements et des logiciels de réseau, mais plutôt d'informer les utilisateurs de systèmes sur les risques posés à la cybersécurité par l'interconnectabilité de ces systèmes. Selon leurs fonctions, rôles ou responsabilités, les utilisateurs doivent avoir une connaissance de base des systèmes auxquels ils peuvent accéder à partir d'autres systèmes et des incidences de leurs actions sur la cybersécurité.

Chaque entité responsable doit s'assurer que tous les membres du personnel auxquels un accès électronique autorisé ou un accès physique autorisé sans accompagnement est accordé à ses *systèmes électroniques BES*, ainsi que les contractuels et les fournisseurs de services, suivent une formation sur la cybersécurité avant d'obtenir cet accès autorisé, sauf dans des *circonstances CIP exceptionnelles*. Pour conserver leur accès autorisé, les personnes doivent suivre la formation au moins une fois tous les 15 mois.

### Exigence E3

Chaque entité responsable doit s'assurer qu'une évaluation des risques liés au personnel est menée pour tout le personnel auquel est accordé un accès électronique autorisé ou un accès physique autorisé sans accompagnement à ses *systèmes électroniques BES*, ainsi que les contractuels et les fournisseurs de services, avant que soit accordé cet accès, exception faite des circonstances exceptionnelles qui ont une incidence sur la fiabilité du *BES* ou la capacité d'intervention d'urgence, qui sont précisées au programme et approuvées par le cadre supérieur désigné ou son délégataire. Le contrôle de l'identité doit être réalisé en respectant les lois fédérales, d'État, provinciales et locales ainsi que les ententes syndicales en vigueur. Ce contrôle n'est nécessaire qu'avant le premier accès à accorder, mais peut être répété périodiquement durant la période d'emploi, selon le processus suivi par l'entité, à l'identique ou d'une autre façon.

Une vérification des antécédents judiciaires sur les sept années précédentes doit être effectuée en tenant compte des endroits où a résidé la personne pendant au moins six mois consécutifs. Cette vérification doit aussi être effectuée en respect des lois fédérales, d'État, provinciales et locales, et est sujette aux conventions collectives en vigueur. S'il est impossible de mener une vérification complète des antécédents judiciaires sur les sept années précédentes, la portion qui a pu être vérifiée doit être documentée ainsi que les motifs pour lesquels la vérification complète sur cette période n'a pu être faite. Il peut s'agir, par exemple, de personnes de moins de 25 ans dont les antécédents à titre de jeune contrevenant sont protégés en vertu de la loi, de personnes qui ont résidé à des endroits où il est impossible d'obtenir des vérifications d'antécédents judiciaires ou de personnes dont l'emploi est régi par une convention collective qui l'interdit. Dans de tels cas, l'entité responsable doit tenir compte du fait que les renseignements sont incomplets lorsqu'elle évalue le risque d'accorder un accès. Chaque

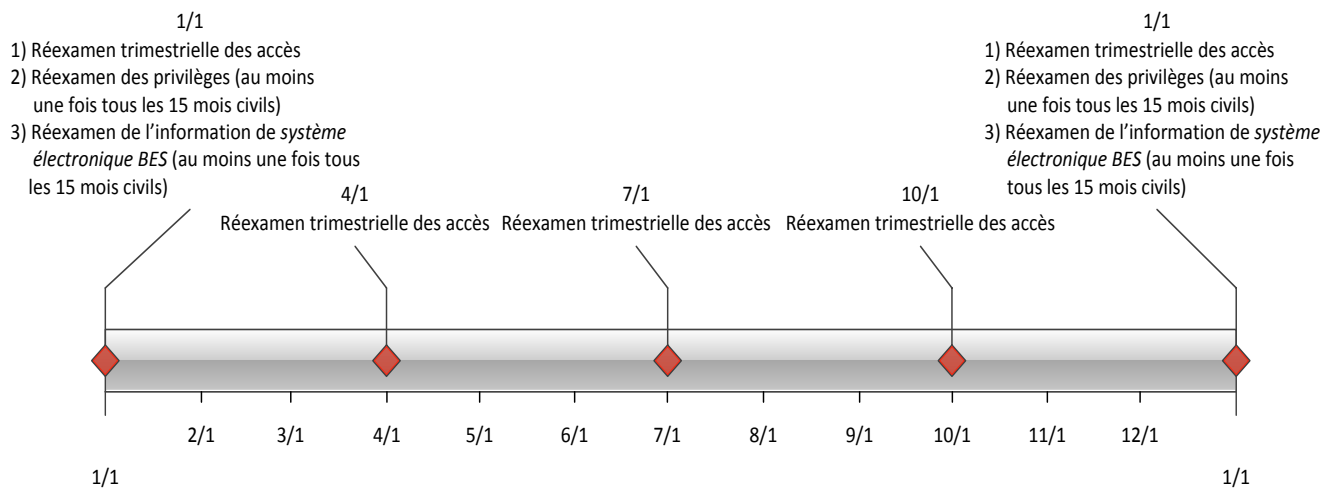
personne ayant un accès doit avoir fait l'objet d'une évaluation des risques liés au personnel au cours des sept années précédentes. Une nouvelle vérification des antécédents judiciaires doit être menée dans le cadre de cette nouvelle évaluation des risques. Les personnes auxquelles on a accordé un accès en vertu d'une version antérieure des présentes normes doivent faire l'objet d'une nouvelle évaluation des risques liés au personnel dans les sept années suivant leur évaluation précédente. Dans la présente version de la norme, le processus de vérification des antécédents judiciaires sur les sept années précédentes a été clarifié de sorte qu'il ne soit pas nécessaire de mener une nouvelle évaluation des risques liés au personnel avant la date de mise en œuvre.

### **Exigence E4**

L'autorisation d'accès électronique et physique sans accompagnement et d'accès à l'information de *système électronique BES* doit être accordée selon le principe du besoin de savoir suivant la fonction de chacun. Les documents attestant l'autorisation doivent comporter une justification des besoins opérationnels invoqués. Pour assurer une séparation adéquate des tâches, l'autorisation et la fourniture d'accès ne doivent pas être assumées par la même personne dans la mesure du possible.

Cette exigence prévoit des réexamens trimestriels ainsi que des réexamens au moins une fois tous les 15 mois civils. Les réexamens trimestriels servent à vérifier que l'accès aux *systèmes électroniques BES* n'a été accordé qu'aux utilisateurs autorisés. Pour ce faire, on compare la liste des personnes ayant reçu un accès à un *système électronique BES* avec le registre des personnes autorisées à accéder à ce *système électronique BES*. Cette exigence met l'accent sur l'intégrité du processus de fourniture d'accès plutôt que sur les comptes individuels de l'ensemble des *actifs électroniques BES*. La liste des personnes ayant reçu un accès peut être une liste de comptes générée automatiquement. Toutefois, dans un *système électronique BES* comptant plusieurs bases de données de comptes, la liste des personnes ayant reçu un accès peut provenir d'autres sources, comme des activités de fourniture d'accès ou d'une base de données de comptes utilisateurs qui sert habituellement de point de départ à la fourniture des accès.

Le réexamen des droits d'accès effectué au moins une fois tous les 15 mois civils est plus détaillé afin de s'assurer que seuls les droits d'accès nécessaires à un utilisateur dans l'exercice de ses fonctions lui soient accordés (droit d'accès minimal). Les entités peuvent optimiser ce réexamen en mettant en place un accès basé sur les rôles. Cette méthode consiste à définir les rôles au sein du système (répartiteur, technicien, récepteur de rapports, administrateur, etc.), puis à grouper les droits d'accès selon ces différents rôles, et enfin à assigner leurs rôles aux utilisateurs. Ce système ne suppose aucun logiciel particulier et on peut le mettre en place en définissant des processus de fourniture d'accès particuliers pour chaque rôle ne permettant pas l'affectation de groupes d'accès. Le système d'autorisation d'accès axé sur les rôles élimine la nécessité d'un réexamen des droits d'accès des comptes individuels. Un calendrier type de tous les réexamens énoncés à l'exigence E4 est illustré ci-dessous.



La séparation des tâches doit être prise en compte au moment de la réalisation des réexamens selon l'exigence E4. La personne chargée du réexamen ne doit pas être celle qui fournit les accès.

Si les résultats des réexamens de comptes trimestriels ou des réexamens de comptes aux 15 mois révèlent qu'il s'est produit une erreur administrative ou de transcription faisant en sorte qu'un accès n'a pas été réellement fourni, la SDT juge que cette erreur ne constitue pas une non-conformité.

Dans le cas de *systèmes électroniques BES* pour lesquels aucun compte utilisateur n'est défini, les contrôles indiqués à l'exigence E4 ne s'appliquent pas. L'entité responsable doit cependant documenter ces configurations.

### Exigence E5

L'exigence de révoquer les accès au moment du départ d'un employé (cessation d'emploi) prévoit des procédures démontrant que la révocation de l'accès se produit en même temps que le départ. On y admet que le moment du départ peut varier selon les circonstances. Quelques scénarios courants et processus possibles selon le moment du départ sont présentés au tableau ci-dessous. Ces scénarios ne constituent pas une liste exhaustive de tous les scénarios possibles, mais ils sont représentatifs de plusieurs pratiques opérationnelles courantes.

Scénario	Processus possible
Départ involontaire immédiat	Un représentant des ressources humaines ou un agent de sécurité accompagne la personne hors du lieu de travail et le superviseur de celle-ci ou le personnel des ressources humaines demande au personnel compétent d'entamer le processus de révocation.

Scénario	Processus possible
Départ involontaire prévu	Le personnel des ressources humaines est avisé du départ et collabore avec le personnel compétent pour que l'accès soit révoqué au moment du départ.
Départ volontaire	Le personnel des ressources humaines est avisé du départ et collabore avec le personnel compétent pour que l'accès soit révoqué au moment du départ.
Départ à la retraite, si le dernier jour de travail est plusieurs semaines avant la date du départ	Le personnel des ressources humaines s'entend avec le gestionnaire sur la date où l'accès ne sera plus nécessaire et planifie la révocation de l'accès pour cette date.
Décès	Le personnel des ressources humaines est avisé du décès et collabore avec le personnel compétent pour entamer le processus de révocation.

On entend par « révocation de l'accès électronique » d'une personne un processus dont le résultat final est l'impossibilité pour elle d'obtenir un accès électronique aux *systèmes électroniques BES* en utilisant les identifiants de connexion qui lui ont été attribués ou qu'elle connaît. Les mesures à prendre pour ce faire comprennent notamment la suppression ou la désactivation des comptes utilisés par cette personne ; aucune mesure précise n'est cependant prescrite dans la norme. Les entités doivent considérer les ramifications d'une suppression de compte, lesquelles peuvent inclure des entrées de journaux d'événements incomplets en raison d'un compte non reconnu ou de services de système utilisant le compte pour se connecter.

La révocation initiale prescrite à l'exigence E5.1 concerne aussi bien l'accès physique non accompagné que l'*accès distant interactif*. La révocation de ces deux accès doit empêcher tout accès de la personne après son départ. Si la personne détient toujours des comptes locaux pour l'accès à des *actifs électroniques BES* (c.-à-d. des comptes spécifiques à ces *actifs électroniques*), l'entité responsable dispose alors de 30 jours pour mener à bien le processus de révocation pour ces comptes. Toutefois, rien n'empêche l'entité responsable de révoquer tous les accès au moment du départ.

Dans le cas d'une personne mutée ou réaffectée, une révision des droits d'accès doit être effectuée. Cette révision peut consister à dresser une simple liste de toutes les autorisations associées à la personne et à travailler en collaboration avec les gestionnaires respectifs pour déterminer de quels accès la personne aura encore besoin dans son nouveau poste. Dans le cas où la personne doit conserver un accès pour une période transitoire, l'entité doit prévoir une date de réexamen de ces droits d'accès ou les inclure dans le réexamen trimestriel des comptes ou le réexamen annuel des droits d'accès.

La révocation de l'accès aux comptes partagés est traitée séparément pour empêcher les situations où les mots de passe des équipements d'un poste ou d'une centrale changeraient constamment en raison du roulement du personnel.

L'exigence 5.5 précise que les mots de passe de comptes partagés doivent être changés dans les 30 jours civils suivant le départ ou lorsque l'entité responsable détermine qu'une personne n'a plus besoin d'avoir accès au compte en raison de sa réaffectation ou de sa mutation. Cette période de 30 jours est valable dans des conditions opérationnelles normales. Toutefois, certaines circonstances peuvent faire en sorte que ce ne soit pas possible. Il peut être nécessaire d'arrêter ou de redémarrer certains systèmes pour compléter le changement de mot de passe. En périodes de chaleur ou de froid extrême, plusieurs entités responsables pourraient interdire l'arrêt et le redémarrage de systèmes afin de maintenir la fiabilité du BES. Dans ce cas, l'entité responsable doit consigner ces circonstances et prévoir changer le mot de passe dans les 10 jours civils suivant la fin de celles-ci. Les documents consignant ces activités doivent être conservés afin de démontrer que l'entité responsable a suivi le plan qu'elle a établi.

### **Justification**

Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

#### **Justification de l'exigence E1 :**

Faire en sorte qu'une entité responsable dont des employés ont un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *actifs électroniques BES* prenne des mesures pour que les employés ayant de tels accès soient toujours au fait de ses pratiques de sécurité.

#### **Justification de l'exigence E2 :**

Faire en sorte que le programme de formation de l'entité responsable à l'intention du personnel ayant besoin d'un accès électronique autorisé ou d'un accès physique autorisé sans accompagnement à des *systèmes électroniques BES* traite des politiques, des contrôles d'accès et des procédures visant à protéger les *systèmes électroniques BES* et que ce personnel reçoive la formation appropriée avant de se voir accorder des accès.

#### **Justification de l'exigence E3 :**

Faire en sorte que les personnes qui ont besoin d'un accès électronique autorisé ou d'un accès physique autorisé sans accompagnement à des *systèmes électroniques BES* ont fait l'objet d'une évaluation des risques. Les personnes qui ont accès à ces systèmes doivent avoir fait l'objet d'une évaluation des risques liés au personnel au cours des sept dernières années, qu'il s'agisse d'une première autorisation d'accès ou du maintien de l'autorisation.

### Justification de l'exigence E4 :

Faire en sorte que les personnes ayant accès à des *systèmes électroniques BES* et à des emplacements physiques et électroniques où l'entité responsable stocke de l'information de *système électronique BES* sont dûment autorisées à avoir accès à ces systèmes et emplacements. L'« autorisation » désigne l'octroi d'une permission par une ou des personnes habilitées par l'entité responsable à autoriser cet octroi ; ce pouvoir fait partie des délégations indiquées à la norme CIP-003-6. La « fourniture » désigne les mesures prises pour fournir un accès à une personne.

L'accès est constitué des accès physique, logique et distant à des *actifs électroniques* qui font partie du *système électronique BES* ou qui permettent l'accès au *système électronique BES*. Au moment d'accorder, de réexaminer ou de révoquer un accès, l'entité responsable doit tenir compte de l'*actif électronique* en particulier de même que des systèmes utilisés pour permettre cet accès (système de contrôle des accès physiques, système d'accès distant, services d'annuaire, etc.).

Les *circonstances CIP exceptionnelles* doivent être définies dans une politique de l'entité responsable conformément à la norme CIP-003-6 ; elles constituent une exception à l'exigence d'autorisation d'accès aux *systèmes électroniques BES* et à l'information de *système électronique BES*.

Les réexamens trimestriels prescrits à l'alinéa 4.5 servent à confirmer que l'accès aux *systèmes électroniques BES* n'a été accordé qu'aux utilisateurs autorisés. Pour ce faire, on compare la liste des personnes auxquelles on a réellement fourni un accès à un *système électronique BES* avec le registre des personnes autorisées à accéder à ce *système électronique BES*. Cette exigence met l'accent sur l'intégrité du processus de fourniture d'accès plutôt que sur les comptes individuels de l'ensemble des *actifs électroniques BES*. La liste des personnes auxquelles on a fourni un accès peut provenir d'une liste de comptes générée automatiquement. Toutefois, dans un *système électronique BES* comptant plusieurs bases de données de comptes, cette liste peut provenir d'autres sources, comme des activités de fourniture d'accès ou d'une base de données de comptes utilisateurs qui sert habituellement de point de départ à la fourniture des accès.

Si les résultats des réexamens de comptes trimestriels ou annuels révèlent qu'il s'est produit une erreur administrative ou de transcription faisant en sorte que l'accès n'a pas été réellement fourni, la SDT juge que cette erreur ne constitue pas une non-conformité.

Dans le cas de *systèmes électroniques BES* pour lesquels aucun compte utilisateur n'est défini, les contrôles indiqués à l'exigence E4 ne s'appliquent pas. L'entité responsable devrait cependant documenter ces configurations.

### Justification de l'exigence E5 :

La révocation rapide de l'accès électronique aux *systèmes électroniques BES* constitue un élément essentiel de tout système de gestion des accès. Lorsque l'accès d'une personne à un *système électronique BES* n'est plus nécessaire dans le cadre de ses fonctions, il doit être révoqué. Cela est particulièrement important dans les situations où des personnes sont licenciées ou réaffectées contre leur gré, puisqu'il y a un risque qu'elles réagissent de manière hostile ou destructrice.

En examinant la manière de répondre aux directives de l'ordonnance 706 de la FERC qui stipulent que l'accès doit être « immédiatement » révoqué en cas de départ involontaire, la SDT a choisi de ne pas préciser de délais en heures dans l'exigence (p. ex. « révoquer l'accès dans l'heure suivant le départ »). Le moment du départ d'une personne ne peut généralement pas être déterminé à l'heure près. Cependant, la plupart des organisations disposent d'un processus de cessation d'emploi en bonne et due forme, et la révocation de l'accès est plus expéditive si elle survient en même temps que les premières étapes de ce processus.

L'accès est constitué des accès physique, logique et distant à des *actifs électroniques* qui font partie du *système électronique BES* ou qui permettent l'accès au *système électronique BES*. Au moment d'accorder, de réexaminer ou de révoquer un accès, l'entité responsable doit tenir compte de l'*actif électronique* en particulier de même que des systèmes utilisés pour permettre cet accès (système de contrôle des accès physiques, système d'accès distant, services d'annuaire, etc.).

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

## A. Introduction

1. **Titre :** Cybersécurité — Personnel et formation
2. **Numéro :** CIP-004-6
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 au Québec :

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 20xx

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 20xx

5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec :

Norme	Entité	Dates d'implantation aux États-Unis	Date d'entrée en vigueur proposée au Québec		Justification
			Impacts moyen et élevé	Impacts faible	
• CIP-004-6	Entités visées par la version 1 des normes CIP adoptées par la Régie.	2016-07-01	2017-07-01	2017-07-01	Uniformisation des pratiques avec les autres juridictions.
	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes.		2018-10-01	2019-10-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
	Entités qui possèdent des installations de production à vocation industrielle		2019-04-01	2020-04-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.

La norme doit être mise en vigueur en même temps que l'ajout des termes de glossaire « actif électronique transitoire » et « support d'information de stockage ».

**6. Contexte :** Aucune disposition particulière

**B. Exigences et mesures**

Aucune disposition particulière

## C. Conformité

### 1. Processus de surveillance de la conformité

#### 1.1. Responsable des mesures pour assurer la conformité

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

#### 1.2. Processus de surveillance de la conformité et d'évaluation de la conformité

Aucune disposition particulière

#### 1.3. Conservation des données

Aucune disposition particulière

#### 1.4. Autres informations sur la conformité

Aucune disposition particulière

### 2. Tableau des éléments de conformité

Aucune disposition particulière

## D. Différences régionales

Aucune disposition particulière

## E. Interprétations

Aucune disposition particulière

## F. Documents connexes

Aucune disposition particulière

## Principes directeurs et fondements techniques

Aucune disposition particulière

## Justification

Aucune disposition particulière

## Historique des versions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	xx mois 201x		Nouvelle