A. Introduction

1. **Titre :** Cybersécurité — Personnel et formation

2. **Numéro :** CIP-004-5.1

3. **Objet :** Minimiser les risques de compromissions, qui pourraient entraîner un fonctionnement incorrect ou une instabilité du BES, 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 systèmes, *installations* 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* qui est 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* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est 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* (excluant les systèmes 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.

   4.1.2.4. 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* qui est 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 par 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* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est 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* (excluant les systèmes 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-002-5 :

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 composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme 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 :

1. **24 mois minimum**– La norme CIP-004-5.1 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-004-5.1 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La norme CIP-004-5.1 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à habiliter l'industrie à identifier, à évaluer et à corriger les lacunes dans la mise en œuvre de certaines exigences. L'intention est de changer la manière de considérer les infractions dans ces exigences, de sorte qu'il ne s'agisse plus de savoir *si* une lacune existe, mais plutôt d'identifier, d'évaluer et de corriger les lacunes. Ceci est présenté dans ces exigences en modifiant la notion de « mise en œuvre » de la façon suivante :

> Chaque entité responsable doit mettre en œuvre**, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes…**

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 devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes. Les processus documentés eux-mêmes n'ont pas à intégrer la démarche « détecter, évaluer et corriger les lacunes » décrite au paragraphe précédent, car cette démarche est liée à la manière de mettre en œuvre les processus documentés et pourrait être réalisée par d'autres mesures de contrôle ou de gestion de la conformité.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela a du sens et est communément compris. 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 un exemple trouvé dans les normes. La mise en œuvre complète des normes 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 de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste 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 *système de production-transport d'électricité*. Un examen des tolérances de 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. Le 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 », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.

- **Systèmes électroniques BES à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.

- **Systèmes électroniques BES à impact moyen à connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. Exclut les *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'événement et d'alerte.

- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès physique*s 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, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-004-5.1) – Programme de sensibilisation à la sécurité. *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]*

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-004-5.1) – 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-004-5.1) – Programme de sensibilisation à la sécurité

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

E2. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou des programmes de formation sur la cybersécurité axée sur les rôles, les fonctions ou les responsabilités de chacun, qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-004-5.1) – Programme de formation sur la cybersécurité. *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]*

M2. Les pièces justificatives doivent inclure les programmes de formation qui comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-004-5.1) – Programme de formation sur la cybersécurité, ainsi que des pièces justificatives additionnelles pour démontrer la mise en œuvre des programmes.

Tableau E2 (CIP-004-5.1) – Programme de formation sur la cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à connectivité externe routable et leurs : 1. EACMS associés ; et 2. PACS associés.	Formation portant sur : 2.1.1. les politiques de cybersécurité ; 2.1.2. le contrôle des accès physiques ; 2.1.3. le contrôle des accès électroniques ; 2.1.4. le programme de contrôle des visiteurs ; 2.1.5. la gestion et le stockage de l'information des *systèmes électroniques BES* ; 2.1.6. la détection des *incidents de cybersécurité* et l'envoi des avis initiaux conformément au plan d'intervention en cas d'incident de l'entité ; 2.1.7. les plans de rétablissement des *systèmes électroniques BES* ; 2.1.8. l'intervention en cas d'*incident de cybersécurité* ; et 2.1.9. les risques pour la cybersécurité associés à l'interconnectabilité et à l'interopérabilité des *systèmes électroniques BES* avec d'autres *actifs électroniques*.	Exemples non limitatifs de pièces justificatives : matériel de formation, tel que présentations PowerPoint, notes à l'intention des instructeurs ou des étudiants, ou documents de cours.

Tableau E2 (CIP-004-5.1) – Programme de formation sur la cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Exige d'avoir terminé la formation énoncée à la partie 2.1 avant de se voir accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *actifs électroniques* visés, sauf dans des *circonstances CIP exceptionnelles*.	Exemples non limitatifs de pièces justificatives : registres de formation et documents attestant l'invocation de *circonstances CIP exceptionnelles*.
2.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS ; et 2. PACS.	Exige d'avoir terminé la formation énoncée à la partie 2.1 au moins une fois tous les 15 mois civils.	Exemple non limitatif de pièce justificative : registres de formation individuels datés.

E3. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs programmes documentés d'évaluation des risques liés au personnel avant d'accorder ou de maintenir un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *systèmes électroniques BES* et qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel. *[Facteur de risque de la 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, comprennent toutes les parties d'exigence applicables du tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre du ou des programmes.

Tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Processus pour confirmer l'identité.	Exemple non limitatif de pièce justificative : documents démontrant le processus suivi par l'entité responsable pour confirmer l'identité.

Tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Processus de vérification des antécédents judiciaires sur les sept années précédentes dans le cadre de chaque évaluation des risques liés au personnel qui comprend : 3.2.1. le lieu où réside actuellement la personne, peu importe depuis combien de temps ; et 3.2.2. les autres endroits où, au cours des sept années précédant immédiatement la date de vérification des antécédents judiciaires, la personne a résidé pendant au moins six mois consécutifs. S'il est impossible de mener une vérification complète des antécédents judiciaires sur les sept années précédentes, pousser la vérification le plus loin possible et consigner les motifs pour lesquels la vérification complète sur cette période n'a pu se faire.	Exemple non limitatif de pièce justificative : documents démontrant le processus suivi par l'entité responsable pour vérifier les antécédents criminels sur les sept dernières années.

Tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Critères ou processus pour évaluer les résultats de la vérification des antécédents judiciaires en vue d'autoriser un accès.	Exemple non limitatif de pièce justificative : documents démontrant le processus de l'entité responsable pour évaluer les résultats des vérifications des antécédents judiciaires.
3.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Critères ou processus pour vérifier que les évaluations des risques liés au personnel dont les entrepreneurs et les fournisseurs de services doivent faire l'objet sont menées conformément aux parties 3.1 à 3.3.	Exemples non limitatifs de pièces justificatives : documents démontrant les critères ou le processus de l'entité responsable pour vérifier les évaluations des risques liés au personnel pour les entrepreneurs et les fournisseurs de services.

Tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.5	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Processus permettant de s'assurer que les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement ont fait l'objet d'une évaluation des risques liés au personnel conformément aux parties 3.1 à 3.4 au cours des sept dernières années.	Exemples non limitatifs de pièces justificatives : documents démontrant 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, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs programmes documentés de gestion des accès qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E4 (CIP-004-5.1) – Programme de gestion des accès. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation du jour même]*

M4. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E4 (CIP-004-5.1) – Programme de gestion des accès, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre des mesures du programme de gestion des accès selon la colonne Mesures du tableau.

Tableau E4 (CIP-004-5.1) – Programme de gestion des accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Processus d'autorisation selon les besoins, tel que déterminé par l'entité responsable, sauf dans des *circonstances CIP exceptionnelles*, de : 4.1.1. l'accès électronique ; 4.1.2. l'accès physique sans accompagnement dans un *périmètre de sécurité physique* ; et 4.1.3. l'accès à des emplacements de stockage (physiques ou électroniques) désignés pour l'information de *système électronique BES*.	Exemples non limitatifs de pièces justificatives : documents datés démontrant le processus suivi pour autoriser un accès électronique, un accès physique sans accompagnement à un *périmètre de sécurité physique* et un accès à des emplacements de stockage (physiques ou électroniques) désignés pour l'information de *système électronique BES*.

Tableau E4 (CIP-004-5.1) – Programme de gestion des accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Vérifier, au moins une fois par trimestre civil, que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d'accès autorisé.	Exemples non limitatifs de pièces justificatives : • documents datés attestant l'établissement d'une comparaison entre la liste, générée par le système, des personnes pour lesquelles on a autorisé l'accès (c.-à-d., base de données des activités de fourniture) et la liste, générée par le système, des personnes ayant un accès (c.-à-d., liste des comptes utilisateurs) ; ou • documents datés attestant l'établissement d'une comparaison entre la liste des personnes pour lesquelles on a autorisé l'accès (c.-à-d., formulaires d'autorisation) et la liste des personnes auxquelles on a fourni un accès (c.-à-d., formulaires de fourniture d'accès ou liste des comptes partagés).

Tableau E4 (CIP-004-5.1) – Programme de gestion des accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Dans le cas d'un accès électronique, vérifier, au moins une fois tous les 15 mois civils, que tous les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont correctement attribués et qu'ils sont ceux jugés nécessaires par l'entité responsable.	Exemples non limitatifs de pièces justificatives : documentation de l'examen, y compris tous les éléments suivants : 1. liste datée de tous les comptes ou groupes de comptes ou rôles au sein du système ; 2. description sommaire des droits d'accès associés à chaque groupe ou rôle ; 3. comptes attribués au groupe ou au rôle ; et 4. preuve datée démontrant que l'on a vérifié que les droits d'accès du groupe sont autorisés et qu'ils sont appropriés selon les fonctions de toute personne à qui ils sont attribués.

Tableau E4 (CIP-004-5.1) – Programme de gestion des accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Vérifier, au moins une fois tous les 15 mois civils, que l'accès aux emplacements de stockage (physiques ou électroniques) désignés pour l'information de *système électronique BES* est correctement attribué et qu'il correspond à ce que l'entité responsable juge nécessaire pour les tâches à accomplir.	Exemples non limitatifs de pièces justificatives : documentation de l'examen, y compris tous les éléments suivants : 1. liste datée des autorisations d'accès à l'information de *système électronique BES* ; 2. droits d'accès associés aux autorisations ; et 3. preuve datée démontrant que l'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.

E5. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs programmes documentés de révocation d'accès qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E5 (CIP-004-5.1) – Révocation d'accès. *[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation du jour même et planification de l'exploitation]*

M5. Les pièces justificatives doivent comprendre chacun des programmes documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables figurant dans le tableau E5 (CIP-004-5.1) – Révocation d'accès, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre selon la colonne Mesures du tableau.

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

Tableau E5 (CIP-004-5.1) – Révocation d'accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
5.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 3. EACMS associés ; et 4. PACS associés.	Dans le cas d'une réaffectation ou d'une mutation, révoquer l'accès électronique autorisé aux comptes individuels et l'accès physique sans accompagnement autorisé que l'entité responsable juge non nécessaires avant la fin du jour civil suivant la date que l'entité responsable détermine comme étant celle où la personne n'a plus besoin de cet accès.	Exemples non limitatifs de pièces justificatives : 1. formulaire d'activité ou d'approbation daté attestant l'examen de l'accès logique et physique ; et 2. journaux ou autres preuves attestant que ces personnes ne disposent plus de l'accès que l'entité responsable détermine comme n'étant plus nécessaire.
5.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Dans le cas d'un départ, révoquer l'accès de la personne aux emplacements de stockage désignés pour l'information de *système électronique BES*, qu'ils soient physiques ou électroniques (à moins que l'accès ait déjà été révoqué selon l'exigence E5.1), avant la fin du jour civil suivant la date à laquelle prend effet le départ.	Exemple non limitatif de pièce justificative : formulaire d'activité ou d'approbation attestant le retrait de l'accès aux emplacements physiques ou aux systèmes électroniques désignés pour l'information de *système électronique BES* daté du jour civil suivant le départ, au plus tard.

Tableau E5 (CIP-004-5.1) – Révocation d'accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
5.4	*Systèmes électroniques BES* à impact élevé et leurs : • EACMS associés.	Dans le cas d'un départ, révoquer l'accès aux comptes utilisateurs non partagés de la personne (à moins que l'accès ait déjà été révoqué selon l'exigence E5.1 ou E5.3) dans les 30 jours civils suivant la date à laquelle prend effet le départ.	Exemple non limitatif de pièce justificative : formulaire d'activité ou d'approbation attestant le retrait de l'accès à un *actif électronique BES* ou à une application logicielle 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	*Systèmes électroniques BES* à impact élevé et leurs : • EACMS associés.	Dans le cas d'un départ, changer les mots de passe des comptes partagés connus de l'utilisateur dans les 30 jours civils suivant le départ. Dans le cas d'une réaffectation ou d'une mutation, changer les mots de passe des comptes partagés connus de l'utilisateur dans les 30 jours civils suivant la date que l'entité responsable détermine comme étant celle où la personne n'a plus besoin de cet accès. Si l'entité responsable détermine et documente que cela prendra plus de temps en raison de circonstances opérationnelles atténuantes, changer les mots de passe dans les 10 jours civils suivant la fin de ces circonstances.	Exemples non limitatifs de pièces justificatives : • formulaire d'activité ou d'approbation attestant que le mot de passe a été réinitialisé dans les 30 jours civils suivant le départ ; • formulaire d'activité ou d'approbation attestant que le mot de passe a été réinitialisé dans les 30 jours civils suivant la réaffectation ou la mutation ; ou • documentation des circonstances opérationnelles atténuantes et formulaire d'activité ou d'approbation attestant que le mot de passe a été réinitialisé dans les 10 jours civils suivant la fin de ces circonstances.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

L'entité régionale joue le rôle de responsable des mesures pour assurer la conformité (CEA), à moins que l'entité concernée soit détenue, exploitée ou contrôlée par l'entité régionale. Dans de tels cas, le rôle de CEA est confié à l'ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

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 pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents 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 sur les non-conformités
- Déclarations de non-conformité
- Plaintes

1.4. Autres informations sur la conformité

- Aucune

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			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 en moins de 10 jours civils après le début d'un trimestre calendrier 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 calendrier subséquent. (1.1)	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait à l'intérieur du trimestre subséquent, mais plus de 30 jours suivant le début de ce trimestre civil. (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 pour au moins deux trimestres civils. (1.1)
E2	**Planification de l'exploitation**	**Faible**	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas inclus un des thèmes de formation dans les parties 2.1.1 à 2.1.9 de l'exigence, et	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas inclus deux des thèmes de formation dans les parties 2.1.1 à 2.1.9 de l'exigence, et	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas inclus trois des thèmes de formation dans les parties 2.1.1 à 2.1.9 de l'exigence, et	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 chacun. (E2)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			n'a pas identifié, évalué et corrigé les lacunes. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas formé une personne (à l'exception des *circonstances CIP exceptionnelles*) avant de lui accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement, et n'a pas identifié, évalué et corrigé les lacunes. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a	n'a pas identifié, évalué et corrigé les lacunes. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas formé deux personnes (à l'exception des *circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement, et n'a pas identifié, évalué et corrigé les lacunes. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la	n'a pas identifié, évalué et corrigé les lacunes. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas formé trois personnes (à l'exception des *circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement, et n'a pas identifié, évalué et corrigé les lacunes. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la	OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas inclus quatre ou plus des thèmes de formation dans les parties 2.1.1 à 2.1.9 de l'exigence, et n'a pas identifié, évalué et corrigé les lacunes. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas formé quatre personnes ou plus (à l'exception des *circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			pas formé une personne avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de complétion de la formation précédente, et n'a pas identifié, évalué et corrigé les lacunes. (2.3)	cybersécurité, mais n'a pas formé deux personnes avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de complétion de la formation précédente, et n'a pas identifié, évalué et corrigé les lacunes. (2.3)	cybersécurité, mais n'a pas formé trois personnes avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de complétion de la formation précédente, et n'a pas identifié, évalué et corrigé les lacunes. (2.3)	autorisé ou un accès physique autorisé sans accompagnement, et n'a pas identifié, évalué et corrigé les lacunes. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas formé quatre personnes ou plus avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de complétion de la formation précédente, et n'a pas identifié, évalué et corrigé les lacunes. (2.3)
E3	**Planification de**	**Moyen**	L'entité responsable a un programme	L'entité responsable a un programme	L'entité responsable a un programme	L'entité responsable n'a pas inclus tous les

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
	l'exploitation		d'évaluation des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et fournisseurs de service, mais n'a pas effectué la PRA comme condition pour accorder l'accès électronique autorisé ou un accès physique autorisé sans accompagnement pour une personne, et n'a pas identifié, évalué et corrigé les lacunes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique	d'évaluation des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et fournisseurs de service, mais n'a pas effectué la PRA comme condition pour accorder l'accès électronique autorisé ou un accès physique autorisé sans accompagnement pour deux personnes, et n'a pas identifié, évalué et corrigé les lacunes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique	d'évaluation des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et fournisseurs de service, mais n'a pas effectué la PRA comme condition pour accorder l'accès électronique autorisé ou un accès physique autorisé sans accompagnement pour trois personnes, et n'a pas identifié, évalué et corrigé les lacunes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique	éléments requis comme indiqué en 3.1 à 3.4 dans les programmes documentés d'évaluation des risques liés au personnel (PRA), pour les personnes, incluant les contractuels et les fournisseurs de service, pour l'obtention et la maintenance des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement. (E3) OU L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et fournisseurs de service, mais n'a pas effectué la PRA comme condition

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			autorisé sans accompagnement, mais n'a pas confirmé l'identité d'une personne, et n'a pas identifié, évalué et corrigé les lacunes. (3.1 et 3.4) OU L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas inclus les vérifications exigées indiquées en 3.2.1 et 3.2.2 pour un personne, et n'a pas	autorisé sans accompagnement, mais n'a pas confirmé l'identité de deux personnes, et n'a pas identifié, évalué et corrigé les lacunes. (3.1 et 3.4) OU L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas inclus les vérifications exigées indiquées en 3.2.1 et 3.2.2 pour deux personnes, et n'a pas	autorisé sans accompagnement, mais n'a pas confirmé l'identité de trois personnes, et n'a pas identifié, évalué et corrigé les lacunes. (3.1 et 3.4) OU L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas inclus les vérifications exigées indiquées en 3.2.1 et 3.2.2 pour trois personnes, et n'a pas	pour accorder l'accès électronique autorisé ou un accès physique autorisé sans accompagnement pour quatre personnes ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas confirmé l'identité de quatre personnes ou plus, et n'a pas identifié, évalué et corrigé les

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			identifié, évalué et corrigé les lacunes. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas évalué la vérification des antécédents judiciaires pour l'autorisation d'accès pour une personne, et n'a pas identifié, évalué et corrigé les lacunes. (3.3 et 3.4) OU	identifié, évalué et corrigé les lacunes. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas évalué la vérification des antécédents judiciaires pour l'autorisation d'accès pour deux personnes, et n'a pas identifié, évalué et corrigé les lacunes. (3.3 et 3.4) OU	identifié, évalué et corrigé les lacunes. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas évalué la vérification des antécédents judiciaires pour l'autorisation d'accès pour trois personnes, et n'a pas identifié, évalué et corrigé les lacunes. (3.3 et 3.4) OU	lacunes. (3.1 et 3.4) OU L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas inclus les vérifications exigées indiquées en 3.2.1 et 3.2.2 pour quatre personnes ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (3.2 et 3.4) OU L'entité responsable a effectué des

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			L'entité responsable n'a pas effectué des évaluations des risques liés au personnel (PRA) pour une personne avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement à l'intérieur de 7 années civiles de la date de complétion de la PRA précédente, et n'a pas identifié, évalué et corrigé les lacunes. (3.5)	L'entité responsable n'a pas effectué des évaluations des risques liés au personnel (PRA) pour deux personnes avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement à l'intérieur de 7 années civiles de la date de complétion de la PRA précédente, et n'a pas identifié, évalué et corrigé les lacunes. (3.5)	L'entité responsable n'a pas effectué des évaluations des risques liés au personnel (PRA) pour trois personnes avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement à l'intérieur de 7 années civiles de la date de complétion de la PRA précédente, et n'a pas identifié, évalué et corrigé les lacunes. (3.5)	évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas évalué la vérification des antécédents judiciaires pour l'autorisation d'accès pour quatre personnes ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (3.3 et 3.4) OU L'entité responsable n'a pas effectué des évaluations des risques liés au personnel (PRA) pour quatre personnes ou plus avec un accès électronique autorisé

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						ou un accès physique autorisé sans accompagnement à l'intérieur de 7 années civiles de la date de complétion de la PRA précédente, et n'a pas identifié, évalué et corrigé les lacunes. (3.5)
E4	**Planification de l'exploitation et exploitation du jour même**	**Moyen**	L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur ont des registres d'autorisation pendant un trimestre civil, mais l'a fait moins de 10 jours civils après le début d'un trimestre civil subséquent, et n'a pas identifié, évalué et corrigé les lacunes. (4.2) OU	L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur ont des registres d'autorisation pendant un trimestre civil, mais l'a fait entre 10 et 20 jours civils après le début d'un trimestre civil subséquent, et n'a pas identifié, évalué et corrigé les lacunes. (4.2)	L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur ont des registres d'autorisation pendant un trimestre civil, mais l'a fait entre 20 et 30 jours civils après le début d'un trimestre civil subséquent, et n'a pas identifié, évalué et corrigé les lacunes. (4.2)	L'entité responsable n'a pas mis en œuvre un programme documenté pour la gestion des accès. (E4) OU L'entité responsable a mis en œuvre un ou plusieurs programmes documentés pour la gestion des accès qui comprennent un processus pour autoriser l'accès électronique, l'accès physique sans accompagnement, ou

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			L'entité responsable a mis en œuvre des processus pour vérifier 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, dans les 15 mois civils suivant la vérification précédente, mais pour 5 % ou moins de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.3) OU L'entité responsable a mis en œuvre des processus pour vérifier que l'accès aux emplacements de	OU L'entité responsable a mis en œuvre des processus pour vérifier 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, dans les 15 mois civils suivant la vérification précédente, mais pour plus de 5 % et moins de (ou égal à) 10 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.3) OU L'entité responsable a	OU L'entité responsable a mis en œuvre des processus pour vérifier 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, dans les 15 mois civils suivant la vérification précédente, mais pour plus de 10 % et moins de (ou égal à) 15 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.3) OU L'entité responsable a	l'accès aux emplacements de stockage désignés où est située l'information de *système électronique BES*, et n'a pas identifié, évalué et corrigé les lacunes. (4.1) OU L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur ont des registres d'autorisation pendant deux trimestres civils consécutifs ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (4.2) OU L'entité responsable a mis en œuvre des

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			stockage pour l'information de *système électronique BES* est correct et nécessaire, dans les 15 mois civils suivant la vérification précédente, mais pour 5 % ou moins de ses emplacements de stockage de l'information de *système électronique BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.4)	mis en œuvre des processus pour vérifier que l'accès aux emplacements de stockage pour l'information de *système électronique BES* est correct et nécessaire, dans les 15 mois civils suivant la vérification précédente, mais pour plus de 5 % et moins de (ou égal à) 10 % de ses emplacements de stockage de l'information de *système électronique BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.4)	mis en œuvre des processus pour vérifier que l'accès aux emplacements de stockage pour l'information de *système électronique BES* est correct et nécessaire, dans les 15 mois civils suivant la vérification précédente, mais pour plus de 10 % et moins de (ou égal à) 15 % de ses emplacements de stockage de l'information de *système électronique BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.4)	processus pour vérifier 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, dans les 15 mois civils suivant la vérification précédente, mais pour plus de 15 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.3) OU L'entité responsable a mis en œuvre des processus pour vérifier que l'accès aux emplacements de stockage pour l'information de

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						système électronique BES est correct et nécessaire, dans les 15 mois civils suivant la vérification précédente, mais pour 15 % ou plus de ses emplacements de stockage de l'information de *système électronique BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.4)
E5	**Exploitation du jour même et planification de l'exploitation**	**Moyen**	L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès de la personne aux emplacements de stockage désignés pour l'information de système électronique BES, mais pour une personne, ne l'a pas	L'entité responsable a mis en œuvre un ou plusieurs processus pour retirer la capacité d'accès physique sans accompagnement et d'*accès distant interactif* lors d'un départ ou pour compléter le retrait dans les 24 heures du	L'entité responsable a mis en œuvre un ou plusieurs processus pour retirer la capacité d'accès physique sans accompagnement et d'*accès distant interactif* lors d'un départ ou pour compléter le retrait dans les 24 heures du	L'entité responsable n'a mis en œuvre aucun programme documenté pour la révocation des accès pour les accès électroniques, les accès physiques sans accompagnement, ou pour les emplacements de stockage des

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			fait avant la fin du jour civil suivant la date et l'heure à laquelle prend effet le départ, et n'a pas identifié, évalué et corrigé les lacunes. (5.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès de la personne aux comptes utilisateurs lors du départ, mais ne l'a pas fait dans les 30 jours civils suivant la date du départ pour une personne ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (5.4) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour changer les mots	départ, mais n'a pas déclenché ces retraits pour une personne, et n'a pas identifié, évalué et corrigé les lacunes. (5.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer qu'une personne n'a plus besoin de conserver les 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 de la personne et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée, et n'a pas identifié, évalué et	départ, mais n'a pas déclenché ces retraits pour deux personnes, et n'a pas identifié, évalué et corrigé les lacunes. (5.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer qu'une personne n'a plus besoin de conserver les 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 de la personne et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée, et n'a pas identifié, évalué et	informations de *système électronique BES*. (E5) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour retirer la capacité d'accès physique sans accompagnement et d'*accès distant interactif* lors d'un départ ou pour compléter le retrait dans les 24 heures du départ, mais n'a pas déclenché ces retraits pour trois personnes ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (5.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			de passe pour les comptes partagés connus de l'utilisateur lors du départ, de la réaffectation ou de la mutation, mais ne l'a pas fait dans les 30 jours civils suivant la date du départ, de la réaffectation ou de la mutation pour une personne ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (5.5) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer et documenter les circonstances opérationnelles atténuantes suivant un départ, une réaffectation ou une mutation, mais n'a pas changé un ou plusieurs	corrigé les lacunes. (5.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès de la personne aux emplacements de stockage désignés pour l'information de système électronique BES, mais pour deux personnes, ne l'a pas fait avant la fin du jour civil suivant la date et l'heure à laquelle prend effet le départ, et n'a pas identifié, évalué et corrigé les lacunes. (5.3)	corrigé les lacunes. (5.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès de la personne aux emplacements de stockage désignés pour l'information de système électronique BES, mais pour trois personnes ou plus, ne l'a pas fait avant la fin du jour civil suivant la date et l'heure à laquelle prend effet le départ, et n'a pas identifié, évalué et corrigé les lacunes. (5.3)	qu'une personne n'a plus besoin de conserver les 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 de la personne et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée, et n'a pas identifié, évalué et corrigé les lacunes. (5.2)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			mots de passe pour des comptes partagés connus de l'utilisateur dans les 10 jours civils suivant la fin des circonstances opérationnelles atténuantes, et n'a pas identifié, évalué et corrigé les lacunes. (5.5)			

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

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 » est 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, alors les normes CIP sur la cybersécurité de la NERC s'appliquent. Il est à noter qu'il y a une restriction à la section 4.1 qui limite l'applicabilité dans le cas des distributeurs 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 qualifiée à la section 4.1, qui est visée par les exigences de la norme. Tel qu'indiqué à la section exemption 4.2.3.5, cette norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou à impact moyen selon la catégorisation de la CIP-002-5. 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* » du glossaire de la NERC comprenne déjà la caractéristique 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 établit quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1 :

Le programme de sensibilisation à la sécurité se veut un programme informatif et non un programme de formation officiel. 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'est pas tenue de fournir des documents qui attestent que chaque personne a reçu ou compris l'information, mais elle doit conserver en tout temps le matériel du programme utilisé, sous forme d'affiches, de notes de service ou de présentations.

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

- communications ciblées (p. ex., courriels, notes de service, formation en ligne, etc.) ;
- communications générales (p. ex., affiches, intranet, brochures, etc.) ;
- rappels et soutien de la direction (p. ex., 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*, et inclure, 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 se composer de plusieurs modules et modes de prestation, mais un seul programme de formation pour toutes les personnes devant être formées est aussi acceptable. L'entité responsable peut, à sa guise, axer la formation sur les fonctions, les rôles ou les responsabilités.

L'ordonnance 706 de la FERC, paragraphe 434, intègre à la formation un nouvel élément qui concerne le matériel et les logiciels de mise en réseau ainsi que les autres éléments d'interconnectabilité électronique nécessaires à l'exploitation et au contrôle des *systèmes électroniques BES*. Cet élément n'exige pas que l'on donne une formation technique aux personnes responsables du matériel et des logiciels de mise en réseau, mais plutôt que l'on informe les utilisateurs de systèmes des 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*, y compris les entrepreneurs et les fournisseurs de services, suivent une formation sur la cybersécurité avant de se voir accorder 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*, y compris les entrepreneurs et les fournisseurs de services, avant que leur soit accordé cet accès, exception faite des circonstances exceptionnelles qui ont une incidence sur la fiabilité du BES ou l'intervention d'urgence, qui sont précisées au programme et approuvées par le cadre supérieur désigné ou son délégué. Le contrôle de l'identité doit être réalisé en respectant les lois fédérales et provinciales et 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'états, 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 se faire. Il peut s'agir, par exemple, de personnes âgées 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 de vérifications des antécédents judiciaires ou des 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 ans 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.

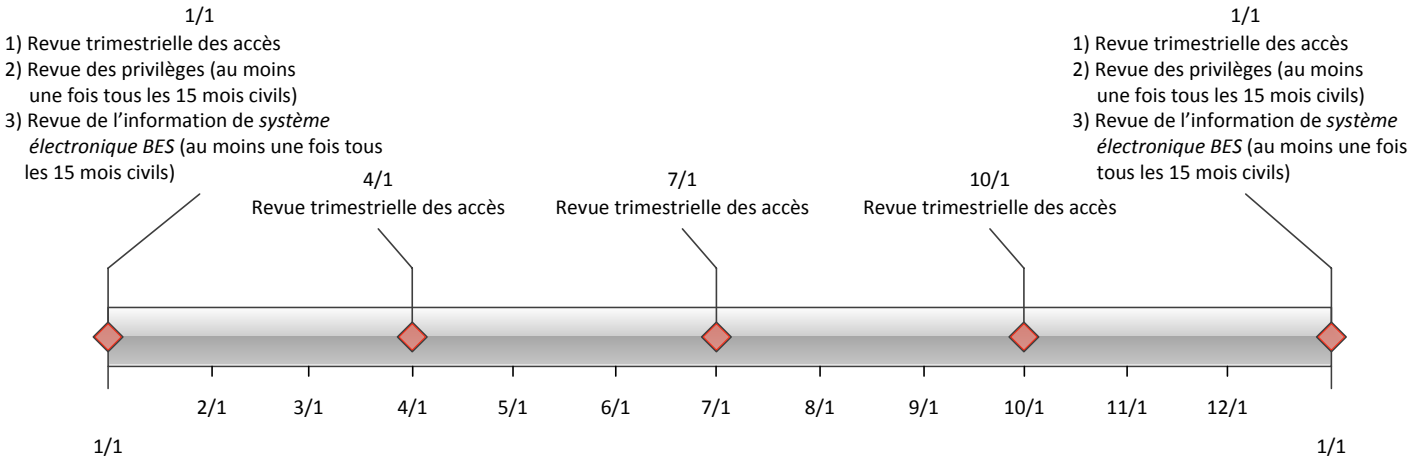
Exigence E4

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 d'affaires 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 examens trimestriels ainsi que des examens au moins une fois tous les 15 mois civils. Les examens 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.

L'examen 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 cet examen en mettant en place un accès basé sur les rôles. Ceci consiste à définir les rôles au sein du système (p. ex., répartiteur, technicien, récepteur de rapports, administrateur, etc.), puis à grouper les droits d'accès selon ces différents rôles, et 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 examen des droits d'accès des comptes individuels. Un calendrier type de tous les examens



énoncés à l'exigence E4 est illustré ci-dessous.

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

Si les résultats des examens de comptes trimestriels ou des examens 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, le 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 d'un départ prévoit des procédures démontrant que la révocation de l'accès se produit en même temps que le départ. On y admet que le moment où l'emploi prend fin peut varier selon les circonstances. Quelques scénarios courants et processus possibles en fonction du moment où cesse l'emploi 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.
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, lorsque le dernier jour de travail est plusieurs semaines avant la date de cessation	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 » un processus dont le résultat final est l'impossibilité d'obtenir un accès électronique aux *systèmes électroniques BES* en utilisant les identifiants de connexion attribués à ou connus de la personne dont les droits d'accès sont révoqués. 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 prescrit 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 à accès local (c.-à-d. des comptes sur l'actif électronique même) sur les *actifs électroniques BES*, 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 impliquer une simple liste de toutes les autorisations associées à la personne et travailler en collaboration avec les gestionnaires respectifs pour déterminer de quels accès elle aura toujours 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 d'examen de ces

droits d’accès ou les inclure dans l’examen de comptes trimestriel ou l’examen 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 changent constamment en raison du roulement du personnel.

L’exigence 5.5 précise que les mots de passe pour comptes partagés doivent être changés dans les 30 jours civils suivant la cessation de l’emploi 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 ces circonstances. Les documents consignant ces activités doivent être conservés afin de démontrer que l’entité responsable a suivi le plan qu’elle a établi.

Raisonnement

Pendant l'élaboration de cette norme, les références aux versions antérieures des normes CIP et le raisonnement derrière les exigences et leurs parties étaient intégrés à même la norme. Sur approbation du BOT, cette information a été déplacée à la présente section.

Raisonnement pour E1 :

Faire en sorte que l'entité responsable avec du personnel ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *actifs électroniques BES* prenne des mesures pour que ce personnel avec de tels accès électroniques autorisés ou accès physiques autorisés sans accompagnement soit toujours au fait de ses pratiques de sécurité.

Sommaire des modifications : Restructuration sous forme de tableau.

Référence à une version précédente : (Partie 1.1) CIP-004-4, E1

Justification des modifications : (Partie 1.1)

Modifications visant à remplacer la nécessité de s'assurer ou de prouver que toutes les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement « ont reçu » un rappel de façon continue énonçant que les pratiques de sécurité ont fait l'objet d'un rappel.

Déplacement des mécanismes de rappel dans les exemples.

Raisonnement pour 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 avant de se voir accorder des accès.

Selon leur rôle, certains membres du personnel n'ont pas nécessairement à être formés sur tous les points.

Sommaire des modifications :

1. Ajout de formation axé sur les rôles pour :

- le programme de contrôle des visiteurs ;
- l'interconnectabilité électronique nécessaire à l'exploitation et au contrôle des *systèmes électroniques BES* ;
- les supports de stockage utilisés pour gérer l'information de *système électronique BES*.

2. Remplacement du terme « *actifs électroniques critiques* » par « *systèmes électroniques BES* ».

Référence une la version précédente : (Partie 2.1) CIP-004-4, E2.2.1

Justification des modifications : (Partie 2.1)

Retrait du concept d'« utilisation adéquate des *actifs électroniques critiques* » des versions antérieures pour mettre l'accent sur les questions de cybersécurité plutôt que sur la fonction administrative. La version précédente mettait l'accent sur l'utilisation administrative ou fonctionnelle des *systèmes électroniques BES*, qui sort du cadre de la cybersécurité. Le personnel qui administre le programme de contrôle des visiteurs ou qui accompagne les visiteurs doit recevoir une formation sur le programme. Formation de base sur la gestion de l'information de *système électronique BES* (et non d'*actif électronique critique*), et ajout du stockage ; ordonnance 706 de la FERC, paragraphe 413 et paragraphes 632 à 634, 688, 732 à 734 ; DHS 2.4.16. Formation de base sur la détection et la déclaration des incidents de cybersécurité ; ordonnance 706 de la FERC, paragraphe 413 ; se reporter à la norme CIP-008-5 et aux exigences de déclaration des incidents du Department of Homeland Security (DHS) pour les personnes ayant un rôle à jouer dans la déclaration des incidents. Formation de base sur les plans d'intervention et les procédures visant à rétablir les *systèmes électroniques BES* qui est donnée au personnel ayant un rôle à jouer dans le rétablissement ; ordonnance 706 de la FERC, paragraphe 413. Les programmes de formation de base sont destinés à englober le matériel et les logiciels de mise en réseau ainsi que sur les autres questions d'interconnectabilité électronique qui soutiennent l'exploitation et le contrôle des *systèmes électroniques BES* ; ordonnance 706 de la FERC, paragraphe 434.

Référence à une version précédente : (Partie 2.2) CIP-004-4, E2.1

Justification des modifications : (Partie 2.2)

L'ajout de critères relatifs aux circonstances exceptionnelles, conformément à l'ordonnance 706 de la FERC, paragraphe 431, est décrit en détail à la norme CIP-003-5.

Référence à une version précédente : (Partie 2.3) CIP-004-4, E2.3

Justification des modifications : (Partie 2.3)

Remplacement de la fréquence « annuelle » par « une fois tous les 15 mois civils ».

Raisonnement pour 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.

Sommaire des modifications : Précise que la vérification des antécédents criminels sur les sept années précédentes doit tenir compte de tous les endroits où a résidé la personne pendant au moins six mois consécutifs, y compris le lieu où elle réside actuellement, peu importe depuis combien de temps.

Référence à une version précédente : (Partie 3.1) CIP-004-4, E3.1

Justification des modifications : (Partie 3.1)

Prise en compte de la demande d'interprétation dans les exemples. Précise qu'il est nécessaire de disposer d'un processus de contrôle de l'identité. Le plan de mise en œuvre précise qu'un contrôle d'identité documenté mené en vertu d'une version antérieure des normes CIP est suffisant.

Référence à une version précédente : (Partie 3.2) CIP-004-4, E3.1

Justification des modifications : (Partie 3.2)

Précise que la vérification des antécédents judiciaires sur les sept années précédentes doit tenir compte de tous les endroits où a résidé la personne pendant au moins six mois, y compris le lieu où elle réside actuellement, peu importe depuis combien de temps. Ajout d'une formulation reposant sur la demande d'interprétation. Modalités pour le cas où il est impossible de mener une vérification complète sur les sept années précédentes.

Référence à une version précédente : (Partie 3.3) Nouvelle

Justification des modifications : (Partie 3.3)

Des critères ou des processus documentés doivent être en place pour permettre une évaluation des résultats des vérifications des antécédents judiciaires en vue d'autoriser un accès.

Référence à une version précédente : (Partie 3.4) CIP-004-4, E3.3

Justification des modifications : (Partie 3.4)

Migration de cette exigence dans sa propre partie d'exigences du tableau.

Référence à une version précédente : (Partie 3.5) CIP-004-3, E3, E3.3

Justification des modifications : (Partie 3.5)

Qu'il s'agisse d'une première autorisation d'accès ou du maintien de l'autorisation, établit que les personnes ayant un accès, doivent avoir fait l'objet d'une évaluation des risques liés au personnel au cours des sept dernières années. Ceci couvre l'initial et de le renouvellement. Le plan de mise en œuvre précise que cette exigence entre en vigueur sept ans après l'évaluation précédente des risques liés au personnel menée en vertu d'une version antérieure des normes CIP sur la cybersécurité. CIP-004-3, E3, E3.3

Raisonnement pour 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 » est considérée comme étant un octroi de permission par une ou des personnes habilitées par l'entité responsable à autoriser cet octroi et faisant partie des délégations mentionnées à la norme CIP 003 5. La « fourniture » devrait être considérée comme étant les mesures prises pour donner un accès à une personne.

L'accès est constitué des accès physiques, logiques, et distant à des *actifs électroniques* qui composent le *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 (p. ex., système de contrôle des accès physiques, système d'accès distant, services d'annuaire).

Les *circonstances CIP exceptionnelles* doivent être définies dans une politique de l'entité responsable conformément à la norme CIP 003 5 ; elles constituent une exception à l'exigence d'autorisation d'accès aux *systèmes électroniques BES* et à l'information de *système électronique BES*.

Les revues trimestrielles énoncées à la partie 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, elle 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 examens 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, le 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.

Sommaire des modifications : La principale modification consiste à rassembler les exigences sur la gestion des accès des normes CIP-003-4, CIP-004-4 et CIP-007-4 en une seule exigence. Les exigences de la version 4 restent pratiquement inchangées, sauf que certains termes ont été clarifiés. En combinant ces exigences, on cherche à ce qu'il n'y ait plus d'impression de redondance entre les processus d'autorisation et d'examen. L'obligation de tenir à jour une liste des employés autorisés, citée dans l'exigence E4 de la norme CIP 004-4, a été éliminée parce que cette liste ne représente qu'une forme de preuve parmi d'autres qui permet de démontrer que seules les personnes autorisées disposent d'un accès.

Références à une version précédente : (Partie 4.1) CIP-003-4, E5.1 et E5.2 ; CIP-006-4, E1.5 et E4 ; et CIP-007-4, E5.1 et E5.1.1

Justification des modifications : (Partie 4.1)

Combinaison des exigences des normes CIP-003-4, CIP-007-4 et CIP-006-4 en vue de clarifier et d'uniformiser le processus d'autorisation. Les normes CIP-003-4, CIP-004-4, CIP-006-4 et CIP-007-4 mentionnent toutes l'autorisation d'accès d'une façon ou d'une autre, et les normes CIP-003-4 et CIP-007-4 stipulent que l'autorisation doit être accordée selon le principe

du besoin de savoir ou selon les fonctions de chacun. Ces exigences ont été combinées afin d'uniformiser la formulation de l'exigence.

Référence à une version précédente : (Partie 4.2) CIP-004-4, E4.1

Justification des modifications : (Partie 4.2)

Les commentaires reçus des membres de l'équipe de rédaction, d'observateurs et d'auditeurs régionaux des normes CIP font état d'une certaine confusion, lors de mise en œuvre des mesures, quant au sens à donner au terme « revoir » à l'exigence E4.1 de la norme CIP-004-4. La présente exigence précise que l'examen doit comparer la fourniture de l'accès et l'autorisation de l'accès.

Référence à une version précédente : (Partie 4.3) CIP-007-4, E5.1.3

Justification des modifications : (Partie 4.3)

Déplacement des exigences pour assurer la cohérence et éliminer les renvois entre exigences. Précision sur les éléments à observer pour effectuer la vérification en indiquant que l'objectif est de confirmer que les droits d'accès sont correctement attribués et qu'ils se limitent au strict minimum.

Référence à la version précédente : (Partie 4.4) CIP-003-4, E5.1.2

Justification des modifications : (Partie 4.4)

Déplacement de l'exigence pour assurer la cohérence entre les examens des autorisations d'accès. Clarification du sens à donner au terme « annuel ». Précision sur les éléments à observer pour effectuer la vérification en indiquant que l'objectif est de confirmer que les droits d'accès sont correctement attribués et qu'ils correspondent au minimum nécessaire pour les tâches à accomplir.

Raisonnement pour 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. Ceci est particulièrement important dans les situations où des personnes sont licenciées ou réaffectées involontairement, 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, le SDT a choisi de ne pas préciser de délais précis dans l'exigence (p. ex., « révoquer l'accès dans l'heure suivant le départ »). Le moment où l'emploi d'une personne prend fin 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 le plus rapide survient en même temps que les premières étapes de ce processus.

L'accès est constitué des accès physiques, logiques, et distant à des *actifs électroniques* qui composent le *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 (p. ex., système de contrôle des accès physiques, système d'accès distant, services d'annuaire).

Sommaire des modifications : L'ordonnance 706 de la FERC, paragraphes 460 et 461, énonce ce qui suit : « La Commission adopte la proposition réglementaire (Notice of Proposed Rulemaking ou NOPR) CIP pour demander à l'organisme de fiabilité du service d'électricité (ERO) d'apporter des modifications à la norme CIP 004 1 afin que soient immédiatement révoqués les droits d'accès d'un employé, d'un entrepreneur ou d'un fournisseur qui n'exerce plus une fonction exigeant un accès physique ou électronique à un *actif électronique critique*, pour quelque raison que ce soit (y compris les mesures disciplinaires, les mutations, les départs à la retraite ou les licenciements).

De façon générale, la Commission est d'avis que la révocation d'un accès dont l'employé n'a plus besoin, en raison d'un changement d'emploi ou d'une cessation d'emploi, doit être immédiate. »

Référence à une version précédente : (Partie 5.1) CIP-004-4, E4.2

Justification des modifications : (Partie 5.1)

L'ordonnance 706 de la FERC, paragraphes 460 et 461, prescrit des modifications aux normes **qui obligent la révocation immédiate** de l'accès de toute personne qui n'en a plus besoin. Pour tenir compte de cette directive, cette exigence stipule que la révocation doit se faire en même temps que la cessation d'emploi, plutôt que dans un délai de 24 heures.

Référence à une version précédente : (Partie 5.2) CIP-004-4, E4.2

Justification des modifications : (Partie 5.2)

L'ordonnance 706 de la FERC, paragraphes 460 et 461, prescrit des modifications aux normes qui obligent la révocation immédiate de l'accès de toute personne qui n'en a plus besoin, y compris les employés mutés. En examinant les modifications à apporter à cette exigence, le SDT a jugé que la date à laquelle une personne n'a plus besoin d'un accès après une mutation posait problème étant donné que les besoins peuvent varier avec le temps. Par conséquent, le SDT a adapté cette exigence à partir de la version 3 de la norme 800-53 du NIST de sorte que l'examen des autorisations d'accès soit fait à la date de mutation. Le SDT a estimé que cette mesure de contrôle permettait d'atteindre plus efficacement l'objectif d'empêcher une personne de cumuler des autorisations inutiles au fil des mutations.

Référence à une version précédente : (Partie 5.3) Nouvelle

Justification des modifications : (Partie 5.3)

L'ordonnance 706 de la FERC, paragraphe 386, prescrit des modifications aux normes qui obligent la révocation rapide de l'accès à l'information protégée. Pour tenir compte de cette directive, les entités responsables doivent révoquer l'accès aux emplacements destinés à

l'information de *système électronique BES.* Ceci pourrait comprendre les classeurs, les salles de commande de postes électriques, les systèmes de gestion des documents, les partages de fichiers ou autres emplacements physiques et logiques sous le contrôle de l'entité responsable.

Référence à une version précédente : (Partie 5.4) Nouvelle

Justification des modifications : (Partie 5.4)

L'ordonnance 706 de la FERC, paragraphes 460 et 461, prescrit des modifications aux normes pour exiger la révocation immédiate de l'accès de toute personne qui n'en a plus besoin. Afin de respecter ce délai immédiat, les entités responsables disposeront probablement de procédures de révocation initiale visant à bloquer l'accès distant et physique au *système électronique BES*. Dans certains cas, la coordination de la révocation d'accès à des *actifs électroniques* et applications individuels peut prendre plus de temps sans nuire à la fiabilité. Cette exigence accorde le délai supplémentaire pour examiner et compléter le processus de révocation. Bien que les mesures initiales empêchent déjà un accès ultérieur, cette étape offre une assurance supplémentaire dans le processus de révocation d'accès.

Référence à la version précédente : (Partie 5.5) CIP-007-4, E5.2.3

Justification des modifications : (Partie 5.5)

Fournir une clarification sur les mesures à prendre pour gérer les mots de passe.

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	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. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsable des mesures pour assurer la conformité ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Approbation par le Conseil d'administration de la NERC.	
3	31 mars 2010	Approbation par la FERC.	
4	30 décembre 2010	Ajout de critères précis pour l'identification des actifs critiques.	Mise à jour
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	Mise à jour
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modifiée en coordination avec les autres normes CIP et révision du format selon le gabarit RBS.
5.1	30 septembre 2013	Modification de deux VSL à E4.	Errata
5.1	22 novembre 2013	Émission d'une ordonnance de la FERC approuvant CIP-004-5.1	
5.1	9 juillet 2014	Émission d'une lettre d'ordonnance approuvant les révisions aux VRF et VSL	L'exigence 4 de CIP-004-5.1 est

		de certaines normes CIP.	passée de Faible à Moyen, et changement des VSL de l'exigence 4 à une gradation basé sur un pourcentage.

Annexe QC-CIP-004-5.1
Dispositions particulières de la norme CIP-004-5.1 applicables au Québec

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-004-5.1

3. Objet : Aucune disposition particulière

4. Applicabilité :

Entités fonctionnelles

Aucune disposition particulière

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 : 29 juillet 2016

5.2. Adoption de l'annexe par la Régie de l'énergie : 29 juillet 2016

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

Pour les entités qui possèdent des actifs classés critiques aux fins des normes CIP (version 1) :

- 1er janvier 2017 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er octobre 2017 pour les systèmes électroniques BES dont l'impact est « faible ».

Pour les entités qui ne possèdent ni des actifs critiques aux fins de normes CIP (version 1), ni des installations de production à vocation industrielle:

- 1er octobre 2018 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er octobre 2019 pour les systèmes électroniques BES dont l'impact est « faible ».

Pour les entités qui possèdent des installations de production à vocation industrielle :

- 1er avril 2019 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er avril 2020 pour les systèmes électroniques BES dont l'impact est « faible ».

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. Conservation des pièces justificatives

Aucune disposition particulière

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

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

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	29 juillet 2016	Nouvelle annexe. Décision D-2016-119 émise par la Régie de l'énergie : • Adoption de la norme et son annexe Québec • Suspension de l'application de la norme et de son annexe Québec pour les entités qui possèdent des installations de production à vocation industrielle	Nouvelle
1	16 septembre 2016	Décision D-2016-138 émise par la Régie de l'énergie reportant la date d'entrée en vigueur en ce qui a trait aux systèmes électroniques BES dont l'impact est « moyen » ou « élevé ».	Révision
2	21 mars 2017	Décision D-2017-031 émise par la Régie de l'énergie : • Levée de suspension d'application de la norme et de son annexe Québec pour les entités qui possèdent des installations de production à vocation industrielle • Fixe la date d'entrée en vigueur pour les entités qui possèdent des installations de production à vocation industrielle.	Révision