Normes de fiabilité

(version française)

A. Introduction

1. Titre : Cybersécurité – Personnel et formation

2. Numéro : CIP-004-7

3. Objet : Réduire au minimum les risques de compromissions susceptibles d'entraîner un fonctionnement incorrect ou une instabilité du *système de production-transport d'électricité* (*BES*) et attribuables à des personnes qui accèdent à des *systèmes électroniques BES,* en exigeant une évaluation des risques liés au personnel, une formation, une sensibilisation à la sécurité et une gestion des accès qui soient adéquates pour protéger ces *systèmes électroniques BES*.

4. Applicabilité :

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

4.1.1. ***Responsable de l'équilibrage***

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

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

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

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

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

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

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

4.1.3. ***Exploitant d'installation de production***

4.1.4. ***Propriétaire d'installation de production***

4.1.5. ***Coordonnateur de la fiabilité***

4.1.6. ***Exploitant de réseau de transport***

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

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

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

4.2.1.1. Système de DSF ou de DST qui :

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

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

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

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

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

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

4.2.3. **Exemptions :** Sont exemptés de la norme CIP-004-7 :

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

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

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

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

4.2.3.5. Les entités responsables qui déterminent n'avoir aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation de la norme CIP-002-5.1a.

5. Dates d'entrée en vigueur : Voir le plan de mise en œuvre de la norme CIP-004-7.

6. Contexte : La norme CIP-004 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES*, ainsi qu'un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

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

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

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

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

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

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

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

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

Colonne « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. La SDT (équipe de rédaction) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en

vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon le processus d'inventaire et de catégorisation de la norme CIP-002-5.1a.
- ***Systèmes électroniques BES* à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon le processus d'inventaire et de catégorisation de la norme CIP-002-5.1a.
- ***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'événements 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, couvrent tous les alinéas applicables du tableau E1 (CIP-004-7) – Programme de sensibilisation à la sécurité.
[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-004-7) – Programme de sensibilisation à la sécurité ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-004-7) – Programme de sensibilisation à la sécurité			
Alinéa	**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 pièces justificatives : 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 des preuves de distribution, notamment : • communications ciblées (p. ex., courriels, notes de service, formation en ligne, etc.) ; • communications générales (p. ex., affiches, intranet, brochures, etc.) ; ou • rappels et soutien de la direction (p. ex., présentations, réunions, etc.).

E2. Chaque entité responsable doit mettre en œuvre un ou des programmes de formation sur la cybersécurité axée sur les rôles, les fonctions ou les responsabilités de chacun, qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-004-7) – Programme de formation sur la cybersécurité.
[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]

M2. Les pièces justificatives doivent comprendre les programmes de formation qui couvrent tous les alinéas applicables du tableau E2 (CIP-004-7) – Programme de formation sur la cybersécurité ; d'autres pièces justificatives doivent attester la mise en œuvre des programmes.

Tableau E2 (CIP-004-7) – Programme de formation sur la cybersécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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*, y compris des *actifs électroniques temporaires*	Exemples non limitatifs de pièces justificatives : matériel de formation comme des présentations PowerPoint, des notes à l'intention des formateurs ou des étudiants, ou des documents de cours.

Tableau E2 (CIP-004-7) – Programme de formation sur la cybersécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
		et des *supports de stockage amovibles*.	
2.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Exiger que soit suivie au complet la formation énoncée à l'alinéa 2.1 avant que soit accordé un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *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 : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Exiger que la formation énoncée à l'alinéa 2.1 soit suivie au complet au moins une fois tous les 15 mois civils.	Exemple non limitatif de pièces justificatives : registres de formation individuels datés.

E3. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés d'évaluation des risques liés au personnel en vue de l'octroi ou du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement à des *systèmes électroniques BES* et qui, collectivement, couvrent tous les parties alinéas applicables du tableau E3 (CIP-004-7) – Programme d'évaluation des risques liés au personnel.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]

M3. Les pièces justificatives doivent comprendre le ou les programmes documentés d'évaluation des risques liés au personnel qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-004-7) – Programme d'évaluation des risques liés au personnel ; d'autres pièces justificatives doivent attester la mise en œuvre du ou des programmes.

Tableau E3 (CIP-004-7) – Programme d'évaluation des risques liés au personnel			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Processus de confirmation de l'identité.	Exemple non limitatif de pièces justificatives : documents attestant le processus suivi par l'entité responsable pour confirmer l'identité.

Tableau E3 (CIP-004-7) – Programme d'évaluation des risques liés au personnel			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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 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 pièces justificatives : documents attestant le processus suivi par l'entité responsable pour vérifier les antécédents criminels sur les sept dernières années.

Tableau E3 (CIP-004-7) – Programme d'évaluation des risques liés au personnel			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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 pièces justificatives : documents attestant le processus de l'entité responsable pour évaluer les résultats des vérifications des antécédents judiciaires.
3.4	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Critères ou processus pour vérifier que les évaluations des risques liés au personnel dont les contractuels et les fournisseurs de services doivent faire l'objet sont menées conformément aux alinéas 3.1 à 3.3.	Exemples non limitatifs de pièces justificatives : documents attestant les critères ou le processus de l'entité responsable pour vérifier les évaluations des risques liés au personnel pour les contractuels et les fournisseurs de services.
3.5	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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 alinéas 3.1 à 3.4 au cours des sept dernières années.	Exemples non limitatifs de pièces justificatives : documents attestant le processus suivi par l'entité responsable pour s'assurer que les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement ont fait l'objet d'une évaluation des risques liés au personnel au cours des sept dernières années.

E4. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de gestion des accès qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-004-7) – Programme de gestion des accès.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation le même jour]

M4. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-004-7) – Programme de gestion des accès ; d'autres pièces justificatives doivent attester la mise en œuvre des mesures du programme de gestion des accès selon la colonne Mesures du tableau.

Tableau E4 (CIP-004-7) – Programme de gestion des accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
4.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Processus d'autorisation selon le besoin déterminé par l'entité responsable, sauf dans des *circonstances CIP exceptionnelles* : 4.1.1. de l'accès électronique ; et 4.1.2. de l'accès physique sans accompagnement dans un *périmètre de sécurité physique*.	Exemples non limitatifs de pièces justificatives : documents datés attestant le processus suivi pour autoriser un accès électronique et un accès physique sans accompagnement à un *périmètre de sécurité physique*.

Tableau E4 (CIP-004-7) – Programme de gestion des accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
4.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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 dossiers d'autorisation.	Exemples non limitatifs de pièces justificatives : • documents datés attestant une comparaison entre la liste automatisée des personnes pour lesquelles on a autorisé l'accès (base de données des activités de fourniture) et la liste automatisée des personnes auxquelles on a fourni un accès (liste des comptes utilisateurs) ; ou • documents datés attestant une comparaison entre la liste des personnes pour lesquelles on a autorisé l'accès (formulaires d'autorisation) et la liste des personnes auxquelles on a fourni un accès (formulaires de fourniture d'accès ou liste des comptes partagés).

Tableau E4 (CIP-004-7) – Programme de gestion des accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
4.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Dans le cas des accès électroniques, vérifier, au moins une fois tous les 15 mois civils, que tous les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont correctement attribués et qu'ils sont ceux jugés nécessaires par l'entité responsable.	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 attestant qu'on a vérifié que les droits d'accès du groupe sont autorisés et qu'ils correspondent aux fonctions de toute personne à qui ils sont attribués.

E5. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de révocation d'accès qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-004-7) – Révocation d'accès.
[Facteur de risque de non-conformité : moyen] [Horizon : exploitation le même jour et planification de l'exploitation]

M5. Les pièces justificatives doivent comprendre chacun des programmes documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-004-7) – Révocation d'accès ; d'autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

Tableau E5 (CIP-004-7) – Révocation d'accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	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 d'accès associé au départ ; et 2. journaux ou autres preuves attestant que la personne ne dispose plus d'un accès.

Tableau E5 (CIP-004-7) – Révocation d'accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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, déterminée par l'entité responsable, où la personne n'a plus besoin de ces accès.	Exemples non limitatifs de pièces justificatives : 1. formulaire d'activité ou d'approbation daté attestant l'examen des accès logique et physique ; et 2. journaux ou autres preuves attestant que la personne ne dispose plus des accès que l'entité responsable détermine comme n'étant plus nécessaires.
5.3	*Systèmes électroniques BES* à impact élevé et : • les *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), 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 un logiciel d'application, selon ce qui est jugé nécessaire pour mener à bien la révocation d'accès, et daté dans les 30 jours civils suivant le départ.

Tableau E5 (CIP-004-7) – Révocation d'accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.4	*Systèmes électroniques BES* à impact élevé et : • les *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, déterminée par l'entité responsable, où la personne n'a plus besoin de cet accès. Si l'entité responsable détermine et documente qu'un délai plus long est nécessaire en raison de circonstances opérationnelles atténuantes, changer les mots de passe dans les 10 jours civils suivant la fin de ces circonstances.	Exemples non limitatifs de pièces justificatives : • formulaire d'activité ou d'approbation attestant que le mot de passe a été changé dans les 30 jours civils suivant le départ ; • formulaire d'activité ou d'approbation attestant que le mot de passe a été changé dans les 30 jours civils suivant la réaffectation ou la mutation ; ou • documentation des circonstances opérationnelles atténuantes et formulaire d'activité ou d'approbation attestant que le mot de passe a été changé dans les 10 jours civils suivant la fin de ces circonstances.

E6. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de gestion des accès afin d'autoriser, de vérifier et de révoquer les accès fournis à des *informations de système électronique BES* (BCSI) relatives aux systèmes désignés à la colonne Systèmes visés du tableau E6 (CIP-004-7) – Gestion des accès aux *informations de système électronique BES*, programmes qui, collectivement, couvrent chacun des alinéas applicables du tableau E6 (CIP-004-7) – Gestion des accès aux *informations de système électronique BES*. Pour être considéré comme ayant accès à des BCSI dans le contexte de cette exigence, une personne doit avoir à la fois la capacité d'obtenir des BCSI et de les utiliser. On considère qu'un accès fourni résulte des mesures prises spécifiquement pour donner à la personne la capacité d'accéder à des BCSI (par exemple, une clé ou une carte d'accès physique, un compte d'utilisateur avec les droits et privilèges connexes, ou une clé de chiffrement).
[Facteur de risque de non-conformité : moyen] [Horizon : exploitation le même jour et planification de l'exploitation]

M6. Les pièces justificatives doivent porter sur chacun des programmes documentés applicables qui, collectivement, couvrent les alinéas applicables du tableau E6 (CIP-004-7) – Gestion des accès aux *informations de système électronique BES* ; d'autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

Tableau E6 (CIP-004-7) – Gestion des accès aux *informations de système électronique BES*

Alinéa	Systèmes visés	Exigences	Mesures
6.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Avant la fourniture de l'accès, autoriser ce qui suit (à moins que l'autorisation soit déjà accordée selon l'alinéa 4.1) selon le besoin déterminé par l'entité responsable, sauf dans des *circonstances CIP exceptionnelles* : 6.1.1 la fourniture d'un accès électronique à des BCSI électroniques ; et 6.1.2 la fourniture d'un accès physique à des BCSI physiques.	Exemples non limitatifs de pièces justificatives : dossiers individuels ou listes indiquant la ou les personnes autorisées, la date d'autorisation et la justification du besoin opérationnel de l'accès fourni.

Tableau E6 (CIP-004-7) – Gestion des accès aux *informations de système électronique BES*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
6.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Vérifier au moins une fois tous les 15 mois civils que toutes les personnes auxquelles un accès à des BCSI a été fourni : 6.2.1 ont toujours un dossier d'autorisation ; et 6.2.2 ont encore besoin de l'accès fourni pour accomplir leur travail, selon l'évaluation de l'entité responsable.	Exemples non limitatifs de pièces justificatives : documentation de l'examen, y compris tous les éléments suivants : • liste de personnes autorisées ; • liste de personnes auxquelles on a fourni un accès ; • confirmation que l'accès fourni est approprié pour le besoin ; et • mesures de réconciliation documentées, s'il y a lieu.
6.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Dans le cas du départ d'une personne, lui retirer la capacité d'utiliser l'accès fourni à des BCSI (à moins que l'accès ait déjà été révoqué selon l'alinéa 5.1), avant la fin du jour civil suivant la date à laquelle prend effet le départ.	Exemples non limitatifs de pièces justificatives : documents de révocation d'accès liés aux départs et datés au plus tard du jour civil suivant le départ.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-004-7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	**Planification de l'exploitation**	**Faible**	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait moins de 10 jours civils après le début d'un trimestre civil subséquent. (1.1)	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait entre 10 et 30 jours civils après le début d'un trimestre civil subséquent. (1.1)	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait au cours du trimestre civil suivant, plus de 30 jours après le début de ce trimestre. (1.1)	L'entité responsable n'a pas documenté ou mis en œuvre un processus de sensibilisation à la sécurité pour rappeler les pratiques de cybersécurité. (E1) OU L'entité responsable n'a pas rappelé les pratiques de cybersécurité et les pratiques de sécurité physique associées pendant au moins deux trimestres civils consécutifs. (1.1)
E2	**Planification de l'exploitation**	**Faible**	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant un des thèmes de formation des alinéas 2.1.1 à 2.1.9 de l'exigence. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former une personne (sauf en cas de *circonstances CIP*	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant deux des thèmes de formation des alinéas 2.1.1 à 2.1.9 de l'exigence. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former deux personnes (sauf en cas de	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant trois des thèmes de formation des alinéas 2.1.1 à 2.1.9 de l'exigence. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former trois personnes (sauf en cas de	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) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant quatre ou plus des thèmes de formation

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-004-7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			exceptionnelles) avant de lui accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former une personne ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la fin de la dernière formation qu'elle a suivie. (2.3)	*circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former deux personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la fin de la dernière formation qu'elle a suivie. (2.3)	*circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former trois personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la fin de la dernière formation qu'elle a suivie. (2.3)	des alinéas 2.1.1 à 2.1.9 de l'exigence. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former quatre personnes ou plus (sauf en cas de *circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former quatre personnes ou plus ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de fin de la dernière formation qu'elle a suivie. (2.3)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-004-7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E3	**Planification de l'exploitation**	**Moyen**	L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à une personne. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de service) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité d'une personne. (3.1 et 3.4) OU L'entité responsable a un processus de vérification	L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à deux personnes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité de deux personnes. (3.1 et 3.4) OU	L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à trois personnes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité de trois personnes. (3.1 et 3.4) OU	L'entité responsable n'a pas inclus tous les éléments des alinéas 3.1 à 3.4 dans les programmes documentés d'évaluation des risques liés au personnel (PRA) pour les personnes, y compris les contractuels et les fournisseurs de services, en vue de l'obtention et du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement. (E3) OU L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à quatre personnes ou plus. (E3)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-004-7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			des antécédents judiciaires sur les sept années précédentes pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour une personne. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis d'évaluer la vérification des antécédents judiciaires pour l'autorisation d'accès d'une personne. (3.3 et 3.4) OU	L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour deux personnes. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis d'évaluer la vérification des antécédents judiciaires pour	L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour trois personnes. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis d'évaluer la vérification des antécédents judiciaires pour	OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité de quatre personnes ou plus. (3.1 et 3.4) OU L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour quatre personnes ou plus. (3.2 et 3.4)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-004-7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour une personne ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA précédente. (3.5)	l'autorisation d'accès de deux personnes. (3.3 et 3.4) OU L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour deux personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA précédente. (3.5)	l'autorisation d'accès de trois personnes. (3.3 et 3.4) OU L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour trois personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA précédente. (3.5)	OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis d'évaluer la vérification des antécédents judiciaires pour l'autorisation d'accès de quatre personnes ou plus. (3.3 et 3.4) OU L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour quatre personnes ou plus ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA précédente. (3.5)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-004-7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E4	**Planification de l'exploitation et exploitation le même jour**	**Moyen**	L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des dossiers d'autorisation pendant un trimestre civil, mais l'a fait moins de 10 jours civils après le début d'un trimestre civil subséquent. (4.2) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires, mais a constaté que, pour 5 % ou moins de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires. (4.3)	L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des dossiers d'autorisation pendant un trimestre civil, mais l'a fait entre 10 et 20 jours civils après le début d'un trimestre civil subséquent. (4.2) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires, mais a constaté que pour plus de 5 % mais au plus 10 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires. (4.3)	L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des dossiers d'autorisation pendant un trimestre civil, mais l'a fait entre 20 et 30 jours civils après le début d'un trimestre civil subséquent. (4.2) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires, , mais a constaté que pour plus de 10 % mais au plus 15 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires. (4.3)	L'entité responsable n'a pas mis en œuvre un programme documenté pour la gestion des accès. (E4) OU L'entité responsable n'a pas mis en œuvre un ou plusieurs programmes documentés pour la gestion des accès comprenant un processus pour autoriser l'accès électronique ou l'accès physique sans accompagnement. (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 sont consignées dans des dossiers d'autorisation pendant deux trimestres civils consécutifs ou plus. (4.2) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-004-7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						mois civils suivant la vérification précédente que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires, mais a constaté que pour plus de 15 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires. (4.3)
E5	**Exploitation le même jour et planification de l'exploitation**	**Moyen**	L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès des personnes à leurs comptes utilisateurs lors de leur départ, mais la révocation n'a pas été faite dans les 30 jours civils suivant la date du départ pour une personne ou plus. (5.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour changer les mots de passe des comptes partagés connus des	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 mener à bien ce retrait dans les 24 heures suivant le départ, mais a omis de déclencher ce retrait pour une personne. (5.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer qu'une personne n'a plus	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 mener à bien ce retrait dans les 24 heures suivant le départ, mais a omis de déclencher ce retrait pour deux personnes. (5.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer qu'une personne n'a plus	L'entité responsable n'a mis en œuvre aucun programme documenté de révocation d'accès pour les accès électroniques ou des accès physiques sans accompagnement. (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 mener à bien ce retrait dans les 24 heures suivant le

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-004-7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			utilisateurs lors de leur départ, de leur réaffectation ou de leur mutation, mais ce changement n'a pas été fait dans les 30 jours civils suivant la date du départ, de la réaffectation ou de la mutation pour une personne ou plus. (5.4) 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 mots de passe de comptes partagés connus d'un utilisateur dans les 10 jours civils suivant la fin de circonstances opérationnelles atténuantes. (5.4)	besoin de conserver des accès à la suite d'une réaffectation ou d'une mutation, mais, pour une personne, n'a pas révoqué les accès électroniques autorisés aux comptes individuels et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée. (5.2)	besoin de conserver des accès à la suite d'une réaffectation ou d'une mutation, mais, pour deux personnes, n'a pas révoqué les accès électroniques autorisés aux comptes individuels et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée. (5.2)	départ, mais a omis de déclencher ce retrait pour trois personnes ou plus. (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 des accès à la suite d'une réaffectation ou d'une mutation, mais, pour trois personnes ou plus, n'a pas révoqué les accès électroniques autorisés aux comptes individuels et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée. (5.2)
E6	Exploitation le même jour et	Moyen	L'entité responsable a mis en œuvre un ou des programmes conformes à l'alinéa 6.1 de l'exigence E6,	L'entité responsable a mis en œuvre un ou des programmes conformes à l'alinéa 6.1 de l'exigence E6,	L'entité responsable a mis en œuvre un ou des programmes conformes à l'alinéa 6.1 de l'exigence E6,	L'entité responsable n'a mis en œuvre aucun programme documenté de

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-004-7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
	planification de l'exploitation		mais dans le cas d'une personne, n'a pas autorisé la fourniture d'un accès électronique à des BCSI électroniques ou d'un accès physique à des BCSI physiques. (6.1) OU L'entité responsable a effectué la vérification requise à l'alinéa 6.2 de l'exigence E6 plus de 15 mois civils, mais au plus 16 mois civils, après la vérification précédente. (6.2) OU L'entité responsable a mis en œuvre un ou des programmes en vue de retirer la capacité d'utiliser l'accès fourni à des BCSI mais, dans le cas d'une personne, n'a pas réalisé ce retrait dans le délai prescrit à l'alinéa 6.3 de l'exigence E6. (6.3	mais dans le cas de deux personnes, n'a pas autorisé la fourniture d'un accès électronique à des BCSI électroniques ou d'un accès physique à des BCSI physiques. (6.1) OU L'entité responsable a effectué la vérification requise à l'alinéa 6.2 de l'exigence E6 plus de 16 mois civils, mais au plus 17 mois civils, après la vérification précédente. (6.2) OU L'entité responsable a mis en œuvre un ou des programmes en vue de retirer la capacité d'utiliser l'accès fourni à des BCSI mais, dans le cas de deux personnes, n'a pas réalisé ce retrait dans le délai prescrit à l'alinéa 6.3 de l'exigence E6. (6.3)	mais dans le cas de trois personnes, n'a pas autorisé la fourniture d'un accès électronique à des BCSI électroniques ou d'un accès physique à des BCSI physiques. (6.1) OU L'entité responsable a effectué la vérification requise à l'alinéa 6.2 de l'exigence E6 plus de 17 mois civils, mais au plus 18 mois civils, après la vérification précédente. (6.2) OU L'entité responsable a mis en œuvre un ou des programmes en vue de retirer la capacité d'utiliser l'accès fourni à des BCSI mais, dans le cas de trois personnes, n'a pas réalisé ce retrait dans le délai prescrit à l'alinéa 6.3 de l'exigence E6. (6.3)	gestion des accès aux BCSI. (E6) OU L'entité responsable a mis en œuvre un ou des programmes conformes à l'alinéa 6.1 de l'exigence E6, mais dans le cas d'au moins quatre personnes, n'a pas autorisé la fourniture d'un accès électronique à des BCSI électroniques ou d'un accès physique à des BCSI physiques. (6.1) OU L'entité responsable a effectué la vérification requise à l'alinéa 6.2 de l'exigence E6 plus de 18 mois civils après la vérification précédente. (6.2) OU L'entité responsable a mis en œuvre un ou des programmes en vue de retirer la capacité d'utiliser l'accès fourni à des BCSI mais, dans le cas d'au moins quatre personnes, n'a pas réalisé ce retrait dans le

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-004-7)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						délai prescrit à l'alinéa 6.3 de l'exigence E6. (6.3)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Historique des versions

Version	Date	Modification apportée	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center ».	24 mars 2006
2	30 septembre 2009	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 de la surveillance de l'application des normes ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Dans l'exigence E1.6, suppression de la phrase concernant le retrait du service d'un composant ou d'un système aux fins d'essais, en réponse à l'ordonnance de la FERC du 30 septembre 2009.	
3	16 décembre 2009	Approbation par le Conseil d'administration de la NERC.	
3	31 mars 2010	Approbation par la FERC.	
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modification en coordination avec les

			autres normes CIP et révision du format selon le modèle RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-004-5.	
5.1	30 septembre 2013	Modification de deux VSL à l'exigence E4.	Errata
6	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication.
6	12 février 2015	Adoption par le conseil d'administration de la NERC.	Remplace la version adoptée par le conseil d'administration le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux *systèmes électroniques BES* à impact faible.
6	21 janvier 2016	Ordonnance de la FERC approuvant la norme CIP-004-6 (dossier RM15-14-000).	
7	12 août 2021	Adoption par le conseil d'administration de la NERC.	Révision visant à améliorer la fiabilité en rapport avec la gestion par les entités de leurs BCSI.
7	7 décembre 2021	Ordonnance de la FERC approuvant la norme CIP-004-7 (dossier RD21-6-000).	
7	10 décembre 2021	Date d'entrée en vigueur.	1er janvier 2024

A. Introduction

1. Titre : Cybersécurité – Protection des informations

2. Numéro : CIP-011-3

3. Objet : Empêcher tout accès non autorisé aux *informations de système électronique BES* (BCSI) en définissant des exigences de protection des informations visant à prévenir toute compromission pouvant entraîner un fonctionnement incorrect ou une instabilité dans le *système de production-transport d'électricité* (*BES*).

4. Applicabilité :

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

4.1.1 ***Responsable de l'équilibrage***

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

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

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

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

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

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

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

4.1.3 ***Exploitant d'installation de production***

4.1.4 ***Propriétaire d'installation de production***

4.1.5 ***Coordonnateur de la fiabilité***

4.1.6 ***Exploitant de réseau de transport***

4.1.7 ***Propriétaire d'installation de transport***

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

sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1 ***Distributeur*** **:** 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 Système de DSF ou de DST qui :

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

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

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

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

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

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

4.2.3 **Exemptions :** Sont exemptés de la norme CIP-011-3 :

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

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

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

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

4.2.3.5 Les entités responsables qui déterminent n'avoir aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation de la norme CIP-002-5.1a.

5. **Dates d'entrée en vigueur :** Voir le plan de mise en œuvre de la norme CIP-011-3.

6. **Contexte :** La norme CIP-011 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES*, ainsi qu'un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

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

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

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

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

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

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

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

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

Colonne « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. La SDT (équipe de rédaction)

CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon le processus d'inventaire et de catégorisation de la norme CIP-002-5.1a.
- ***Systèmes électroniques BES* à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon le processus d'inventaire et de catégorisation de la norme CIP-002-5.1a.
- ***Systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) –** Désigne tout système *de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification et systèmes de surveillance de registre d'événements et d'alerte.
- ***Systèmes de contrôle des accès physiques* (*PACS*) –** Désigne tout *système de contrôle des accès physique*s associés à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.
- ***Actifs électroniques protégés* (*PCA*) –** Désigne tout *actif électronique protégé* associé à un ***système** électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de protection des *informations de système électronique BES* (BCSI) relatives aux systèmes désignés à la colonne Systèmes visés du tableau E1 (CIP-011-3) – Programme de protection des informations, qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-011-3) – Protection des informations.
[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]

M1. Les pièces justificatives du programme de protection des informations doivent couvrir toutes les parties applicables du tableau E1 (CIP-011-3) – Programme de protection des informations ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-011-3) – Programme de protection des informations			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Méthodes permettant de désigner les BCSI.	Exemples non limitatifs de pièces justificatives acceptables : • méthode documentée permettant de désigner les BCSI à partir du programme de protection des informations de l'entité ; • indications sur les informations (étiquetage, classification, etc.) qui permettent de désigner les BCSI telles que désignées dans le programme de protection des informations de l'entité ; • matériel de formation qui donne au personnel des connaissances suffisantes pour reconnaître les BCSI ; ou • emplacements désignés pour le stockage des BCSI dans le cadre du programme de protection des informations de l'entité.

Tableau E1 (CIP-011-3) – Programme de protection des informations			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Méthodes de protection et de manipulation sécuritaire des BCSI visant à réduire les risques de brèche de confidentialité.	Exemples non limitatifs de pièces justificatives pour les BCSI présentes à l'intérieur du périmètre : • procédures pour la protection et la manipulation sécuritaire des BCSI, portant sur des aspects comme le stockage, la sécurité pendant le transport et l'utilisation ; ou • enregistrements indiquant que les BCSI sont manipulées conformément aux procédures documentées de l'entité. Exemples non limitatifs de pièces justificatives pour les BCSI à l'extérieur du périmètre : • mise en œuvre de techniques électroniques pour protéger les BCSI électroniques (masquage de données, chiffrement, hachage, tokenisation, système de clés électroniques, etc.) ; ou • mise en œuvre de moyens physiques pour protéger les BCSI physiques (verrouillage physique et gestion des clés, système de cartes d'identification, biométrie, système d'alarme, etc.) ; ou • mise en œuvre de méthodes administratives pour protéger les BCSI (évaluation des risques des fournisseurs de services, ententes commerciales, etc.).

E2. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-011-3) – Réutilisation et élimination des *actifs électroniques BES*.
[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]

M2. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent toutes les parties applicables du tableau E2 (CIP-011-3) – Réutilisation et élimination des *actifs électroniques BES* ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-011-3) – Réutilisation et élimination des *actifs électroniques BES* **Alinéa**	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Avant d'autoriser la réutilisation d'un *actif électronique* visé qui contient des BCSI (sauf si cet actif est réutilisé dans d'autres systèmes indiqués à la colonne Systèmes visés), l'entité responsable doit faire en sorte d'empêcher toute récupération non autorisée de BCSI stockées sur le support de stockage de l'*actif électronique* en question.	Exemples non limitatifs de pièces justificatives acceptables : • enregistrements de suivi des mesures d'expurgation visant à empêcher toute récupération non autorisée de BCSI, notamment par écrasement, purge ou destruction ; ou • enregistrements de suivi de mesures comme le cryptage, la rétention dans le *périmètre de sécurité physique* ou d'autres moyens d'empêcher la récupération non autorisée de BCSI.
2.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Avant l'élimination d'un *actif électronique* visé qui contient des BCSI, l'entité responsable doit faire en sorte d'empêcher toute récupération non autorisée de BCSI stockées sur l'*actif électronique* en question, ou encore de détruire son support d'information.	Exemples non limitatifs de pièces justificatives acceptables : • enregistrements attestant que le support d'information a été détruit avant l'élimination d'un *actif électronique* visé ; ou • enregistrements attestant les mesures prises pour empêcher la récupération non autorisée de BCSI d'un *actif électronique* visé avant son élimination.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

Niveaux de gravité de la non-conformité (VSL)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-011-3)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	**Planification de l'exploitation**	**Moyen**	Sans objet	Sans objet	L'entité responsable a documenté mais n'a pas mis en œuvre un ou des programmes de protection des BCSI. (E1) OU L'entité responsable a documenté mais n'a pas mis en œuvre au moins une méthode permettant de désigner les BCSI. (1.1) OU L'entité responsable a documenté mais n'a pas mis en œuvre au moins une méthode de protection et de manipulation sécuritaire des BCSI. (1.2)	L'entité responsable n'a ni documenté ni mis en œuvre de programme de protection des BCSI. (E1)
E2	**Planification de l'exploitation**	**Faible**	Sans objet	L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais n'a pas inclus de processus de réutilisation visant à empêcher la récupération non autorisée de BCSI à partir de l'*actif électronique BES.* (2.1)	L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais n'a pas inclus de processus d'élimination ou de destruction de support afin d'empêcher la récupération non autorisée de BCSI à partir de l'*actif électronique BES.* (2.2)	L'entité responsable n'a documenté ou mis en œuvre aucun processus pour les alinéas applicables du tableau E3 (CIP-011-3) – Réutilisation et élimination des *actifs électroniques BES.* (E2)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	26 novembre 2012	Adoption par le conseil d'administration de la NERC.	Cette norme définit les exigences de protection de l'information en coordination avec d'autres normes CIP et met en œuvre certaines dispositions de l'ordonnance 706 de la FERC.
1	22 novembre 2013	Ordonnance de la FERC approuvant CIP-011-1 (ordonnance entrant en vigueur le 3 février 2014).	
2	13 novembre 2014	Adoption par le conseil d'administration de la NERC.	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication.
2	12 février 2015	Adoption par le conseil d'administration de la NERC.	Remplace la version adoptée par le conseil d'administration le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux *systèmes électroniques BES* à impact faible.
2	21 janvier 2016	Ordonnance de la FERC approuvant la norme CIP-011-2 (dossier RM15-14-000).	

Version	Date	Intervention	Suivi des modifications
3	12 août 2021	Adoption par le conseil d'administration de la NERC.	Révision visant à améliorer la fiabilité en rapport avec la gestion par les entités de leurs BCSI.
3	7 décembre 2021	Ordonnance de la FERC approuvant la norme CIP-011-3 (dossier RD21-6-000).	
3	10 décembre 2021	Date d'entrée en vigueur.	1er janvier 2024