

A. Introduction

1. **Titre :** Cybersécurité — Gestion de la sécurité des systèmes
2. **Numéro :** CIP-007-6
3. **Objet :** Gérer la sécurité des systèmes en établissant des exigences techniques, opérationnelles et administratives particulières afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient 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 des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.
 - 4.1.1 **Responsable de l'équilibrage**
 - 4.1.2 **Distributeur** qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du *BES* :
 - 4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :
 - 4.1.2.1.1 fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et
 - 4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant.
 - 4.1.2.2 Chaque *automatisme de réseau (SPS)* ou *plan de défense (RAS)* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.
 - 4.1.2.3 Chaque *système de protection* applicable au *transport* (à l'exclusion des systèmes DSF et DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.
 - 4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des prochains groupes de production à démarrer.
 - 4.1.3 **Exploitant d'installation de production**
 - 4.1.4 **Propriétaire d'installation de production**

4.1.5 Coordonnateur des échanges ou responsable des échanges**4.1.6 Coordonnateur de la fiabilité****4.1.7 Exploitant de réseau de transport****4.1.8 Propriétaire d'installation de transport**

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

4.2.1.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus au moyen d'un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant.

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

4.2.1.3 Chaque *système de protection* applicable au *transport* (à l'exclusion des 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-007-6 :

4.2.3.1 les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

- 4.2.3.2** les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;
 - 4.2.3.3** les systèmes, structures et composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54 ;
 - 4.2.3.4** dans le cas des *distributeurs*, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;
 - 4.2.3.5** les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* classés dans les catégories « impact élevé » ou « impact moyen » selon le processus de désignation et de catégorisation de la norme CIP-002-5.1.
- 5. Dates d'entrée en vigueur :**
- Voir le plan de mise en œuvre de la norme CIP-007-6.
- 6. Contexte :**
- La norme CIP-007 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.
- La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui couvrent tous les alinéas applicables du tableau [référence au tableau]. » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.
- L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.
- Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », dans la mesure où la compréhension relève du bon sens. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.
- De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation

du personnel sont des exemples qui figurent dans les normes. La mise en œuvre complète des normes de fiabilité CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

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

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

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

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

Colonne « Systèmes visés » des tableaux

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

- ***Systèmes électroniques BES à impact élevé*** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.

- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- **Systèmes électroniques BES à impact moyen de centres de contrôle** – Désigne uniquement les *systèmes électroniques BES* à impact moyen situés dans des *centres de contrôle*.
- **Systèmes électroniques BES à impact moyen à connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à *connectivité externe routable*, à l'exclusion des *actifs électroniques* des *systèmes électroniques BES* auxquels on ne peut avoir accès directement par *connectivité externe routable*.
- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS)** – Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification et systèmes de surveillance de registre d'événements et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès physiques* associé à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.
- **Actifs électroniques protégés (PCA)** – Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

- E1.** Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-007-6) – Ports et services.
[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation le même jour]
- M1.** Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-007-6) – Ports et services ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-007-6) – Ports et services			
Alinéa	Systèmes visés	Exigences	Mesures
1.1	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les EACMS associés ; 2. les PACS associés ; et 3. les PCA associés. <p><i>Systèmes électroniques BES</i> à impact moyen à <i>connectivité externe routable</i> et :</p> <ol style="list-style-type: none"> 1. les EACMS associés ; 2. les PACS associés ; et 3. les PCA associés. 	<p>Si cela est techniquement faisable, activer uniquement les ports logiques accessibles par le réseau qui sont jugés nécessaires par l'entité responsable, y compris les plages de ports ou de services qui sont nécessaires pour la prise en charge de ports dynamiques. Si un dispositif ne permet pas la désactivation ou la restriction de ses ports logiques, tous les ports ouverts sont considérés comme nécessaires.</p>	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • documentation établissant la nécessité de tous les ports activés de tous les <i>actifs électroniques</i> et <i>points d'accès électronique</i> visés, pris individuellement ou collectivement ; • listes des ports d'écoute des <i>actifs électroniques</i>, pris individuellement ou collectivement, provenant des fichiers de configuration des dispositifs, du résultat de commandes comme netstat ou de balayages réseau des ports ouverts ; ou • fichiers de configuration des pare-feu (de type hôte) ou de tout autre mécanisme intégré au matériel qui n'autorisent l'accès qu'aux ports nécessaires et qui le refusent à tous les autres.

Tableau E1 (CIP-007-6) – Ports et services			
Alinéa	Systèmes visés	Exigences	Mesures
1.2	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>PCA</i> associés ; et 2. les composants de communication non programmables associés situés à la fois dans un <i>périmètre de sécurité physique</i> et dans un <i>périmètre de sécurité électronique</i>. <p><i>Systèmes électroniques BES à impact moyen de centres de contrôle et :</i></p> <ol style="list-style-type: none"> 1. les <i>PCA</i> associés ; et les composants de communication non programmables associés situés à la fois dans un <i>périmètre de sécurité physique</i> et dans un <i>périmètre de sécurité électronique</i>. 	Empêcher l'utilisation de ports d'entrée-sortie physiques non nécessaires utilisés pour la connectivité de réseau, les commandes pupitre ou les <i>supports de stockage amovibles</i> .	Exemple non limitatif de pièces justificatives : documentation indiquant le type de protection assurée pour les ports d'entrée-sortie physiques – soit logique (configuration du système), soit physique (verrouillage ou signalisation).

- E2.** Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité.
[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]
- M2.** Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité			
Alinéa	Systèmes visés	Exigences	Mesures
2.1	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés; et 3. les <i>PCA</i> associés. 	Un processus de gestion des correctifs portant sur le suivi, l'évaluation et l'installation des correctifs de cybersécurité pour les <i>actifs électroniques</i> visés. Le suivi comprend la désignation de la ou des sources que l'entité responsable utilise pour faire le suivi de la publication de correctifs de cybersécurité destinées aux <i>actifs électroniques</i> visés qui sont actualisables et pour lesquels il existe une source de correctifs.	Exemples non limitatifs de pièces justificatives : documentation d'un processus de gestion des correctifs et documentation ou listes de sources qui sont utilisées pour le suivi visant chacun des <i>systèmes électroniques BES</i> ou des <i>actifs électroniques BES</i> .

Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité			
Alinéa	Systèmes visés	Exigences	Mesures
2.2	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Au moins une fois tous les 35 jours civils, évaluer l'applicabilité des correctifs de sécurité publiées par la ou les sources indiquées à l'alinéa 2.1 depuis l'évaluation précédente.	Exemple non limitatif de pièces justificatives : une évaluation effectuée ou citée par une entité responsable ou réalisée en son nom et portant sur les correctifs de sécurité publiées par les sources documentées, et ce, au moins tous les 35 jours civils.

Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité

Alinéa	Systèmes visés	Exigences	Mesures
2.3	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	<p>Pour les correctifs jugés applicables selon l'alinéa 2.2, prendre une des mesures suivantes dans les 35 jours civils suivant la fin de l'évaluation :</p> <ul style="list-style-type: none"> • appliquer les correctifs applicables ; • créer un plan d'atténuation daté ; ou • réviser un plan d'atténuation existant. <p>Les plans d'atténuation doivent comprendre les mesures que l'entité responsable compte prendre pour atténuer les vulnérabilités visées par chaque correctif de sécurité, ainsi qu'un délai de mise en œuvre de ces mesures.</p>	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • enregistrements d'installation des correctifs (p. ex. rapport exporté d'un outil automatisé de gestion des correctifs indiquant la date d'installation, validation de la version du logiciel des composants du <i>système électronique BES</i> ou exportation d'un registre indiquant que le logiciel a été installé) ; ou • plan daté indiquant à quel moment et de quelle façon la vulnérabilité sera corrigée, qui documente les mesures que l'entité responsable compte prendre pour atténuer les vulnérabilités visées par la correctif de sécurité et qui précise un délai d'exécution des mesures d'atténuation.

Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité

Alinéa	Systèmes visés	Exigences	Mesures
2.4	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Pour chaque plan d'atténuation créé ou mis à jour selon l'alinéa 2.3, mettre le plan en œuvre dans le délai qui y est précisé, à moins qu'une révision du plan ou un prolongement du délai indiqué à l'alinéa 2.3 soit approuvé par le <i>cadre supérieur CIP</i> ou son délégataire.	Exemple non limitatif de pièces justificatives : registres de mise en œuvre des plans d'atténuation.

- E3.** Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-007-6) – Protection contre les programmes malveillants.
[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation le même jour]
- M3.** Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-007-6) – Protection contre les programmes malveillants ; d’autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E3 (CIP-007-6) – Protection contre les programmes malveillants			
Alinéa	Systèmes visés	Exigences	Mesures
3.1	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Utiliser une ou des méthodes pour bloquer, détecter ou prévenir les programmes malveillants.	Exemple non limitatif de pièces justificatives : suivis de la mise en œuvre de ces méthodes par l’entité responsable (au moyen de logiciels antivirus habituels, du renforcement des systèmes, de politiques, etc.).

Tableau E3 (CIP-007-6) – Protection contre les programmes malveillants			
Alinéa	Systèmes visés	Exigences	Mesures
3.2	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Atténuer la menace des programmes malveillants détectés.	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • registres des processus d'intervention en cas de détection de programmes malveillants ; • suivis de la performance de ces processus lorsque des programmes malveillants sont détectés.
3.3	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Pour les méthodes indiquées à l'alinéa 3.1 qui utilisent des signatures ou des séquences de code, avoir un processus de mise à jour des signatures et des séquences de code. Le processus doit traiter de l'essai et de l'installation des signatures et des séquences de code.	Exemple non limitatif de pièces justificatives : documentation décrivant le processus de mise à jour des signatures et des séquences de code.

- E4.** Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-007-6) – Surveillance des événements de sécurité.
[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation le même jour et évaluation des activités d'exploitation]
- M4.** Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-007-6) – Surveillance des événements de sécurité ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E4 (CIP-007-6) – Surveillance des événements de sécurité			
Alinéa	Systèmes visés	Exigences	Mesures
4.1	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les EACMS associés ; 2. les PACS associés ; et 3. les PCA associés. <p><i>Systèmes électroniques BES à impact moyen et :</i></p> <ol style="list-style-type: none"> 1. les EACMS associés ; 2. les PACS associés ; et 3. les PCA associés. 	<p>Journaliser les événements au niveau du <i>système électronique BES</i> (selon les capacités du <i>système électronique BES</i>) ou au niveau de l'<i>actif électronique</i> (selon les capacités de l'<i>actif électronique</i>) permettant la détection des <i>incidents de cybersécurité</i> – et les enquêtes subséquentes à leur sujet – qui comprennent au minimum chacun des types d'événements suivants :</p> <ol style="list-style-type: none"> 4.1.1. toute tentative détectée d'ouverture de session ayant réussi ; 4.1.2. toute tentative détectée d'accès ou d'ouverture de session ayant échoué ; et 4.1.3. tout programme malveillant détecté. 	<p>Exemples non limitatifs de pièces justificatives : liste des types d'événements que le <i>système électronique BES</i> est en mesure de détecter, générée manuellement ou automatiquement, et, le cas échéant, qu'il est configuré pour journaliser. Cette liste doit comprendre les types d'événements obligatoires.</p>

Tableau E4 (CIP-007-6) – Surveillance des événements de sécurité			
Alinéa	Systèmes visés	Exigences	Mesures
4.2	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	<p>Générer des alertes pour les événements de sécurité qui, selon l'entité responsable, nécessitent une alerte, y compris au minimum chacun des types d'événements suivants (selon les capacités de l'<i>actif électronique</i> ou du <i>système électronique BES</i>) :</p> <ol style="list-style-type: none"> 4.2.1. programmes malveillants détectés conformément à l'alinéa 4.1 ; et 4.2.2. échec détecté de la journalisation des événements définis à l'alinéa 4.1. 	<p>Exemples non limitatifs de pièces justificatives : liste, générée manuellement ou automatiquement, des événements de sécurité qui, selon l'entité responsable, nécessitent des alertes, y compris une liste, générée manuellement ou automatiquement, indiquant la configuration des alertes.</p>

Tableau E4 (CIP-007-6) – Surveillance des événements de sécurité			
Alinéa	Systèmes visés	Exigences	Mesures
4.3	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen de centres de contrôle et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Si cela est techniquement faisable, conserver les journaux des événements exigés à l'alinéa 4.1 pendant au moins 90 jours civils consécutifs, sauf dans des <i>circonstances CIP exceptionnelles</i> .	Exemples non limitatifs de pièces justificatives : documentation du processus de conservation des journaux des événements et rapports générés manuellement ou automatiquement qui indiquent que la configuration de conservation des journaux est réglée à 90 jours ou plus.
4.4	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; et 2. les <i>PCA</i> associés. 	Examiner un résumé ou un échantillon des événements journalisés, tels que définis par l'entité responsable, à intervalles d'au plus 15 jours civils, afin de repérer les <i>incidents de cybersécurité</i> non détectés.	Exemples non limitatifs de pièces justificatives : document décrivant l'examen et ses constatations éventuelles, et document daté démontrant que l'examen a eu lieu.

- E5.** Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes.
[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]
- M5.** Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes			
Alinéa	Systèmes visés	Exigences	Mesures
5.1	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen de centres de contrôle et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Avoir une ou plusieurs méthodes pour imposer l'authentification de tout accès utilisateur interactif, si cela est techniquement faisable.	Exemple non limitatif de pièces justificatives : documentation décrivant le mode d'authentification des accès.

Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes			
Alinéa	Systèmes visés	Exigences	Mesures
5.2	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Répertorier par système, par groupe de systèmes, par emplacement ou par type de système tous les comptes par défaut ou autres comptes génériques qui sont connus et activés.	Exemple non limitatif de pièces justificatives : liste de comptes indiquant les types de comptes activés ou génériques utilisés pour le <i>système électronique BES</i> .
5.3	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Recenser toutes les personnes ayant un accès autorisé à des comptes partagés.	Exemple non limitatif de pièces justificatives : liste des comptes partagés et des personnes qui y ont un accès autorisé.

Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes

Alinéa	Systèmes visés	Exigences	Mesures
5.4	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Changer les mots de passe par défaut connus, selon les capacités de l' <i>actif électronique</i> .	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • documentation de l'exécution d'une procédure selon laquelle les mots de passe sont changés lorsque de nouveaux dispositifs sont en service ; ou • mention dans les manuels des systèmes ou dans d'autres documents de leurs fournisseurs selon laquelle les mots de passe par défaut ont été générés de façon pseudo-aléatoire et sont donc exclusifs à chaque dispositif.

Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes

Alinéa	Systèmes visés	Exigences	Mesures
5.5	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	<p>En ce qui concerne l'authentification uniquement par mot de passe de l'accès utilisateur interactif, imposer les paramètres suivants par des moyens techniques ou procéduraux :</p> <ol style="list-style-type: none"> 5.5.1. une longueur de mot de passe d'au moins huit caractères ou de la longueur maximale permise par l'<i>actif électronique</i>, selon la moindre des deux ; et 5.5.2. une complexité minimale du mot de passe d'au moins trois types différents de caractères (lettres majuscules, lettres minuscules, chiffres, caractères non alphanumériques, etc.) ou du maximum permis par l'<i>actif électronique</i>, selon la moindre des deux. 	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • rapports générés automatiquement ou captures d'écran montrant les paramètres de mot de passe appliqués par le système, y compris la longueur et la complexité ; ou • attestations comportant un renvoi aux procédures documentées ayant été suivies.

Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes

Alinéa	Systèmes visés	Exigences	Mesures
5.6	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	Si cela est techniquement faisable, pour toute authentification uniquement par mot de passe de l'accès utilisateur interactif, imposer par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe au moins une fois tous les 15 mois civils.	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • rapports générés automatiquement ou captures d'écran montrant la fréquence de changement de mot de passe appliquée par le système ; ou • attestations comportant un renvoi aux procédures documentées ayant été suivies.
5.7	<p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES à impact moyen de centres de contrôle et :</i></p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; 2. les <i>PACS</i> associés ; et 3. les <i>PCA</i> associés. 	<p>Si cela est techniquement faisable :</p> <ul style="list-style-type: none"> • limiter le nombre de tentatives d'authentification infructueuses ; ou • générer des alertes après un certain nombre de tentatives d'authentification infructueuses. 	<p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • documentation des paramètres de verrouillage de compte ; ou • règles de configuration des alertes indiquant comment le système avise des personnes après un nombre défini de tentatives d'authentification infructueuses.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

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

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

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

1.3. Processus de surveillance et de mise en application des normes

Audits de conformité

Déclarations sur la conformité

Contrôles ponctuels

Enquêtes de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune.

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	Exploitation le même jour	Moyen	Sans objet	L'entité responsable a mis en œuvre et documenté des processus pour les ports et services, mais n'avait aucune méthode pour empêcher l'utilisation de ports d'entrée-sortie physiques non nécessaires utilisés pour la connectivité de réseau, les commandes pupitre ou les <i>supports de stockage amovibles</i> . (1.2)	L'entité responsable a mis en œuvre et documenté des processus pour déterminer les ports et services nécessaires, mais un ou plusieurs ports logiques accessibles par le réseau et jugés non nécessaires étaient activés même s'il était techniquement faisable de les désactiver. (1.1)	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus parmi les éléments applicables du tableau E1 (CIP-007-6). (E1)
E2	Planification de l'exploitation	Moyen	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour évaluer l'applicabilité des correctifs de sécurité publiés et non installés, mais a évalué l'applicabilité des correctifs de sécurité dans un délai de plus de 35 jours civils et d'au plus 50 jours civils après l'évaluation précédente pour la ou les sources indiquées. (2.2) OU L'entité responsable a un ou plusieurs processus documentés pour l'évaluation des correctifs	L'entité responsable a documenté ou mis en œuvre un ou plusieurs processus pour la gestion des correctifs, mais n'a inclus aucun processus comprenant la désignation de la ou des sources pour le suivi ou l'évaluation des correctifs de cybersécurité destinées aux <i>actifs électroniques</i> visés. (2.1) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour évaluer l'applicabilité des correctifs de sécurité publiés et non	L'entité responsable a documenté ou mis en œuvre un ou plusieurs processus pour la gestion des correctifs, mais n'a inclus aucun processus pour l'installation des correctifs de cybersécurité destinées aux <i>actifs électroniques</i> visés. (2.1) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour évaluer l'applicabilité des correctifs de sécurité publiés et non installés, mais n'a pas évalué l'applicabilité des	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus parmi les éléments applicables du tableau E2 (CIP-007-6). (E2) OU L'entité responsable a documenté ou mis en œuvre un ou plusieurs processus pour la gestion des correctifs, mais n'a inclus aucun processus pour le suivi, l'évaluation ou l'installation des correctifs de cybersécurité destinées aux <i>actifs électroniques</i> visés. (2.1)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			de cybersécurité, mais, afin d'atténuer les vulnérabilités exposées par les correctifs de sécurité applicables, a appliqué les correctifs applicables, créé un plan d'atténuation daté, ou révisé un plan d'atténuation existant dans un délai de plus de 35 jours civils et d'au plus 50 jours civils après la fin de l'évaluation. (2.3)	installées, mais a évalué l'applicabilité des correctifs de sécurité dans un délai de plus de 50 jours civils et d'au plus 65 jours civils après l'évaluation précédente pour la ou les sources indiquées. (2.2) OU L'entité responsable a un ou plusieurs processus documentés pour l'évaluation des correctifs de cybersécurité, mais, afin d'atténuer les vulnérabilités exposées par les correctifs de sécurité applicables, a appliqué les correctifs applicables, créé un plan d'atténuation daté ou révisé un plan d'atténuation existant dans un délai de plus de 50 jours civils et d'au plus 65 jours civils après la fin de l'évaluation. (2.3)	correctifs de sécurité dans les 65 jours civils après l'évaluation précédente pour la ou les sources indiquées. (2.2) OU L'entité responsable a un ou plusieurs processus documentés pour l'évaluation des correctifs de cybersécurité, mais, afin d'atténuer les vulnérabilités exposées par les correctifs de sécurité applicables, n'a pas appliqué les correctifs applicables, créé un plan d'atténuation daté ou révisé un plan d'atténuation existant dans les 65 jours civils après la fin de l'évaluation. (2.3)	OU L'entité responsable a documenté un plan d'atténuation pour une correctif de cybersécurité applicable et a documenté une révision ou un prolongement du délai, mais n'a pas obtenu l'approbation du <i>cadre supérieur CIP</i> ou de son délégué. (2.4) OU L'entité responsable a documenté un plan d'atténuation pour une correctif de cybersécurité applicable, mais n'a pas mis en œuvre le plan tel que créé ou révisé dans le délai spécifié dans le plan. (2.4)
E3	Exploitation le même jour	Moyen	Sans objet	L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais, dans les cas où des signatures ou des séquences de code sont utilisées, l'entité	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour la protection contre les programmes malveillants, mais n'a pas atténué la menace des programmes	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus parmi les éléments applicables du tableau E3 (CIP-007-6). (E3)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				responsable n'a pas traité de l'essai des signatures et des séquences de code. (3.3)	malveillants détectés. (3.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour la protection contre les programmes malveillants, mais, dans les cas où des signatures ou des séquences de code sont utilisées, l'entité responsable n'a pas mis à jour les protections contre les programmes malveillants. (3.3)	OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour la protection contre les programmes malveillants, mais n'a pas déployé de méthodes pour bloquer, détecter ou prévenir les programmes malveillants. (3.1)
E4	Exploitation le même jour et évaluation des activités d'exploitation	Moyen	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les <i>incidents de cybersécurité</i> non détectés en examinant, au moins tous les 15 jours civils, un résumé ou un échantillon des événements journalisés défini par l'entité, mais a raté un intervalle et terminé l'examen dans les 22 jours civils après l'examen précédent. (4.4)	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les <i>incidents de cybersécurité</i> non détectés en examinant, au moins tous les 15 jours civils, un résumé ou un échantillon des événements journalisés défini par l'entité, mais a raté un intervalle et terminé l'examen dans les 30 jours civils après l'examen précédent. (4.4)	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour générer des alertes pour les événements de sécurité nécessaires (selon le jugement de l'entité responsable) pour les systèmes applicables (selon les capacités du dispositif ou du système), mais n'a pas généré d'alertes pour tous les types d'événements indiqués en 4.2.1 à 4.2.2. (4.2) OU	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus parmi les éléments applicables du tableau E4 (CIP-007-6). (E4) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour journaliser les événements pour les systèmes applicables (selon les capacités du dispositif ou du système), mais n'a pas journalisé tous les types d'événements requis

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
					<p>L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour journaliser les événements applicables indiqués en 4.1 (si cela est techniquement faisable et sauf dans des <i>circonstances CIP exceptionnelles</i>), mais n'a pas conservé les journaux d'événements applicables pendant au moins les 90 derniers jours consécutifs. (4.3)</p> <p>OU</p> <p>L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les <i>incidents de cybersécurité</i> non détectés en examinant, au moins tous les 15 jours civils, un résumé ou un échantillon des événements journalisés défini par l'entité, mais a raté deux intervalles ou plus. (4.4)</p>	indiqués en 4.1.1 à 4.1.3. (4.1)
E5	Planification de l'exploitation	Moyen	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas inclus l'inventaire de tous	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs des processus qui couvrent les alinéas applicables du

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			interactif, mais a imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans un délai de plus de 15 mois civils et d'au plus 16 mois civils après le dernier changement de mot de passe. (5.6)	interactif, mais a imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans un délai de plus de 16 mois civils et d'au plus 17 mois civils après le dernier changement de mot de passe. (5.6)	<p>les comptes par défaut ou autres types de comptes génériques qui sont connus et activés, soit par système, par groupe de systèmes, par emplacement ou par type de système. (5.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas inclus le recensement des personnes ayant un accès autorisé à des comptes partagés. (5.3)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur interactif qui n'imposent pas, par des moyens techniques ou procéduraux, un des deux paramètres de mot de passe indiqués en 5.5.1 et 5.5.2. (5.5)</p> <p>OU</p>	<p>tableau E5 (CIP-007-6). (E5)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas de méthodes pour imposer l'authentification de l'accès utilisateur interactif même si c'est techniquement faisable. (5.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas, selon les capacités du dispositif, changé les mots de passe par défaut connus. (5.4)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur interactif qui n'imposent, par des moyens techniques</p>

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
					<p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur interactif, mais a imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans un délai de plus de 17 mois civils et d'au plus 18 mois civils après le dernier changement de mot de passe. (5.6)</p>	<p>ou procéduraux, aucun des paramètres de mot de passe indiqués en 5.5.1 et 5.5.2. (5.5)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur interactif, mais n'a pas imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans un délai de 18 mois civils après le dernier changement de mot de passe. (5.6)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas soit limité le nombre de tentatives d'authentification infructueuses, soit généré des alertes après un certain</p>

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						nombre de tentatives d'authentification infructueuses, même si c'est techniquement faisable. (5.7)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center ».	24 mars 2006
2	30 septembre 2009	<p>Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes.</p> <p>Suppression de la mention sur la prise en compte des considérations d'affaires.</p> <p>Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable.</p> <p>Reformulation de la date d'entrée en vigueur.</p> <p>Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsable des mesures ».</p>	
3	16 décembre 2009	<p>Changement du numéro de version de -2 à -3. Approbation par le Conseil d'administration de la NERC.</p> <p>Dans l'exigence 1.6, suppression de la phrase concernant le retrait du service d'un composant ou d'un système aux fins d'essais, en</p>	

		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.	Remaniement 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-007-5.	
6	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication.
6	12 février 2015	Adoption par le conseil d'administration de la NERC	Remplace la version adoptée par le conseil d'administration le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux <i>systèmes électroniques BES</i> à impact faible.

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

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

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

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

Exigence E1

L'exigence E1 a pour but de réduire la surface d'attaque des *actifs électroniques* en obligeant les entités à désactiver les ports non nécessaires. L'intention de la SDT est de faire en sorte que l'entité sache quels ports et services connexes sont accessibles (« ports d'écoute ») sur ses actifs et systèmes et s'ils sont nécessaires au fonctionnement de l'*actif électronique*, et qu'elle désactive tous les autres ports ou limite l'accès à ceux-ci.

1.1. Le plus souvent, il est possible de respecter cette exigence en désactivant le service ou programme à l'écoute sur le port, ou les paramètres de configuration dans l'*actif électronique*. Il est aussi possible d'utiliser des ordinateurs pare-feu, des enveloppeurs TCP ou d'autres moyens sur l'*actif électronique* afin de restreindre l'accès. À noter : cette exigence s'applique aux *actifs électroniques*, qui constituent les *systèmes électroniques BES* pertinents et les *actifs électroniques* qui leur sont associés. Ce contrôle constitue une autre couche de défense contre les attaques provenant du réseau et, par conséquent, la SDT souhaite que le contrôle soit installé sur le dispositif lui-même ou y soit raccordé directement, sans possibilité de contournement. Le verrouillage de ports à la frontière du *périmètre de sécurité électronique* ne se substitue pas à cette exigence touchant le dispositif. Si un dispositif ne permet pas que l'on en désactive ou restreigne les ports logiques (par exemple, un dispositif spécialement conçu et commandé par micrologiciel, sans configuration de port possible), les ports ouverts sont alors jugés « nécessaires ».

1.2. Les ports d'entrée-sortie physiques sont par exemple les ports réseau, série et USB à l'extérieur du boîtier du dispositif. Puisque les *systèmes électroniques BES* doivent se trouver à l'intérieur d'un *périmètre de sécurité physique*, les ports d'entrée-sortie physiques sont protégés contre les accès non autorisés. Une utilisation accidentelle est cependant possible, par exemple le branchement d'un modem ou d'un câble reliant des réseaux, ou l'insertion d'une clé USB. Les ports utilisés pour les « commandes pupitre » sont principalement des ports série sur des *actifs électroniques* qui fournissent une interface de gestion.

La protection de ces ports peut être assurée par plusieurs moyens, notamment les suivants :

- désactivation de tous les ports physiques non nécessaires dans la configuration de l'*actif électronique* ;
- signalisation bien en évidence, ruban inviolable ou tout autre moyen servant à signaler que les ports ne doivent pas être utilisés sans autorisation appropriée ;
- obstruction des ports physiques au moyen de verrous amovibles.

Les ports réseau visés par cet alinéa de l'exigence ne se limitent pas à ceux du *système électronique BES* lui-même. Les ports réseau physiques comprennent ceux qui peuvent exister dans des dispositifs non programmables comme des commutateurs, des concentrateurs ou des panneaux de répartition non gérés.

Il s'agit d'un contrôle faisant partie d'une démarche de « défense en profondeur » et qui tient compte du fait qu'il existe d'autres niveaux de contrôle, dont le *périmètre de sécurité physique*, qui empêchent le personnel non autorisé d'avoir un accès physique à ces ports. Même avec l'accès physique, il a été souligné qu'il y avait d'autres moyens de contourner le contrôle. Ce type de contrôle, qui comprend notamment la signalisation, ne se veut pas un moyen de prévention contre les intrusions. En effet, la signalisation est un contrôle directif plus qu'un contrôle préventif. Toutefois, dans une approche de défense en profondeur, différents niveaux et types de contrôles sont exigés d'un bout à l'autre de la norme, ce qui renforce la sécurité dans l'environnement des *centres de contrôle*. Une fois que le personnel autorisé a accédé physiquement après avoir satisfait aux autres mesures de prévention et de détection, il est opportun de prévoir comme dernière ligne de défense dans ces secteurs à très haut risque un contrôle directif décrivant le comportement approprié. Essentiellement, la signalisation sert à rappeler aux utilisateurs autorisés de réfléchir avant de brancher quoi que ce soit sur un de ces systèmes : c'est exactement ce que vise cette exigence. Ce contrôle n'est pas conçu principalement pour empêcher les intrusions, mais plutôt à l'intention d'un employé autorisé, par exemple, qui voudrait brancher son téléphone intelligent possiblement infecté sur le port USB du pupitre d'un répartiteur afin d'en recharger la pile.

La colonne Systèmes visés de l'alinéa 1.2 de l'exigence E1 a été modifiée dans la version CIP-007-6, de manière à s'appliquer aux « composants de communication non programmables associés situés à la fois dans un *périmètre de sécurité physique* et dans un *périmètre de sécurité électronique* ». Sont ainsi visés uniquement les composants de communication non programmables qui sont situés dans un *périmètre de sécurité physique* et aussi dans un

périmètre de sécurité électronique, et non les composants situés dans un seul périmètre, comme l'illustre le schéma suivant :

Location of nonprogrammable communication components	Emplacement des composants de communication non programmables
PSP	Périmètre de sécurité physique
ESP	Périmètre de sécurité électronique
Applicability of CIP-007-6 R1, Part 1.2 for nonprogrammable communication components	Applicabilité de l'alinéa 1.2 de l'exigence E1 de la norme CIP-007-6 aux composants de communication non programmables

Exigence E2

L'intention de la SDT en produisant l'exigence E2 est d'obliger les entités à se tenir au courant des vulnérabilités logicielles connues qui sont associées à leurs *actifs électroniques BES*, à en faire le suivi et à en atténuer les effets. Il ne s'agit pas de leur imposer l'installation de chaque correctif de sécurité, mais plutôt d'exiger qu'ils se tiennent au courant de toutes les vulnérabilités connues et de les gérer en temps opportun.

La gestion des correctifs de sécurité s'impose pour les *systèmes électroniques BES* qui sont accessibles à distance et pour les systèmes autonomes. Ces derniers sont vulnérables à l'introduction intentionnelle ou involontaire de programmes malveillants. Une solide stratégie de défense en profondeur emploie des mesures supplémentaires telles que la sécurité physique, un logiciel de protection contre les programmes malveillants et la gestion des correctifs pour restreindre l'introduction de programmes malveillants ou l'exploitation de vulnérabilités connues.

Un ou plusieurs processus peuvent être utilisés. Par exemple, un processus d'évaluation global peut être abordé dans un document principal, des documents secondaires établissant le processus plus détaillé à suivre pour chacun des systèmes. Ces documents secondaires peuvent notamment aborder les caractéristiques particulières des *systèmes électroniques BES*.

2.1. L'entité responsable doit disposer d'un programme de gestion des correctifs qui aborde le suivi, l'évaluation et l'installation des correctifs de cybersécurité. Cette exigence s'applique uniquement aux correctifs de sécurité, c'est-à-dire aux correctifs publiés pour corriger une vulnérabilité particulière dans un produit matériel ou logiciel. Ainsi, elle ne concerne que les correctifs permettant de corriger des problèmes de cybersécurité et exclut les correctifs uniquement liées à la fonctionnalité sans répercussions sur la cybersécurité. Le suivi comprend des processus par lesquels l'entité est avisée de la disponibilité de nouvelles correctifs de cybersécurité pertinentes pour les *actifs électroniques*. La documentation de la source de correctifs est exigée à l'étape de suivi pour déterminer à quel moment commence la période d'évaluation. Cette exigence tient compte des situations où un correctifs de sécurité peut provenir d'une première source (comme un fournisseur de systèmes d'exploitation), mais qu'elle doit être approuvée ou certifiée par une autre source (comme un fournisseur de

systèmes de contrôle) avant de pouvoir être évaluée et appliquée sans compromettre la disponibilité ou l'intégrité du système de contrôle. La source peut prendre plusieurs formes : la « National Vulnerability Database » du NIST et les fournisseurs de systèmes d'exploitation ou de systèmes de contrôle peuvent tous être des sources pour le suivi de la publication de correctifs de sécurité, de correctifs et de mises à jour. Une source de correctifs n'est pas obligatoire pour les *actifs électroniques* qui n'ont pas de logiciel ou de micrologiciel actualisable (les utilisateurs ne peuvent pas mettre à jour le logiciel interne ou un micrologiciel s'exécutant sur l'*actif électronique*) ou pour lesquels il n'existe pas de source de correctifs, par exemple quand le fournisseur n'existe plus. La détermination de ces sources n'est nécessaire qu'une seule fois, à moins qu'un logiciel change ou qu'il soit ajouté à la configuration de référence de l'*actif électronique*.

2.2. Les entités responsables doivent effectuer une évaluation des correctifs de sécurité dans les 35 jours civils suivant leur publication par la source suivie. L'évaluation doit consister à déterminer l'applicabilité de chaque à l'environnement et aux systèmes propres à l'entité. Cela consiste principalement à vérifier si le correctif s'applique à un composant logiciel ou matériel particulier que l'entité a installé dans un *actif électronique* visé. Une correctif conçue pour un service ou un composant qui n'est pas installé dans l'environnement de l'entité n'est pas pertinente. Si l'entité détermine que la correctif est non pertinente, il lui suffit de le documenter et de le justifier pour être conforme. Si la correctif est pertinente, l'évaluation peut comprendre une détermination du risque couru, la façon de remédier à la vulnérabilité, l'urgence et le délai de mise en œuvre de la mesure corrective, de même que les démarches déjà entreprises par l'entité ou qu'elle compte entreprendre. Lorsque des *systèmes électroniques BES* ou des *actifs électroniques BES* ne sont plus pris en charge par leurs fournisseurs, il faut faire très attention avant d'y appliquer des correctifs de sécurité, des correctifs ou des mises à jour ou des mesures de neutralisation. Il est en effet possible que des correctifs, des correctifs et des mises à jour réduisent la fiabilité du système, et les entités doivent en tenir compte en choisissant les mesures de neutralisation à prendre. Les entités responsables peuvent utiliser l'information fournie dans le document *Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems* du Department of Homeland Security (DHS). Le document *Recommended Practice for Patch Management of Control Systems* du DHS fournit des lignes directrices relatives au processus d'évaluation. Ce document propose des niveaux de gravité déterminés au moyen du « Common Vulnerability Scoring System » (version 2). Une exception liée à la faisabilité technique (TFE) n'est pas indiquée lorsqu'il est déterminé qu'un correctif ou une mise à jour représente un trop grand risque pour un système ou n'est pas pertinent en raison de la configuration du système.

Au moment de documenter les mesures correctives, il n'est peut-être pas nécessaire de les consigner une par une. Le plan de mesures correctives peut être cumulatif. Par exemple, pour s'attaquer à une vulnérabilité d'un logiciel, l'entité peut choisir de désactiver un service particulier. Or, comme ce service peut être ciblé pour exploiter d'autres vulnérabilités du logiciel, sa désactivation permet de neutraliser plusieurs vulnérabilités.

2.3. Cette exigence tient compte des situations où le déploiement d'une correctif visant une vulnérabilité représente un plus grand risque pour la fiabilité d'un système en exploitation que

la vulnérabilité elle-même. Dans tous les cas, l'entité a le choix soit d'installer la correctif, soit de documenter, au moyen d'un nouveau plan d'atténuation ou de la mise à jour d'un plan existant, ce qu'elle entend faire pour atténuer la vulnérabilité et à quel moment elle compte le faire. Il est parfois plus judicieux, pour protéger la fiabilité, de ne pas installer une correctif, auquel cas l'entité peut consigner les mesures qu'elle a prises pour atténuer la vulnérabilité. Lorsque des correctifs de sécurité sont jugés pertinentes, l'entité responsable doit, dans les 35 jours civils, les installer, créer un plan d'atténuation daté qui décrit les mesures à prendre ou celles qu'elle a déjà prises pour atténuer les vulnérabilités visées par les correctifs de sécurité, ou réviser un plan d'atténuation existant. Le délai fixé ne doit pas nécessairement être un jour civil en particulier, mais peut être désigné par un événement comme « le prochain arrêt planifié d'au moins deux jours ». Les plans d'atténuation dont il est question dans la présente norme désignent des documents internes et ne doivent pas être confondus avec les plans d'atténuation soumis aux entités régionales en réponse aux non-conformités.

2.4. L'entité a été avisée d'un risque connu, l'a évalué, a mis au point un plan pour y remédier et doit ensuite mettre en œuvre ce plan. Un plan de remédiation qui comprend seulement des mesures déjà mises en œuvre est considéré comme ayant été mis en œuvre dès que la documentation du plan est terminée. Un plan de remédiation comportant des mesures à prendre pour remédier à la vulnérabilité doit être mis en œuvre selon l'échéance que l'entité a indiquée dans le plan. L'exigence ne prescrit pas de délai maximal, car l'application de correctifs et la modification des systèmes comportent leurs propres risques pour la disponibilité et l'intégrité des systèmes et peuvent devoir être reportées jusqu'au moment d'un arrêt planifié. Lors des périodes de forte demande ou de conditions météorologiques menaçantes, la modification des systèmes peut être réduite ou refusée à cause du risque pour la fiabilité.

Exigence E3

3.1. Étant donné la vaste gamme d'équipements composant les *systèmes électroniques BES*, la grande variété des fonctions de ces équipements et de leurs vulnérabilités aux maliciels, ainsi que l'évolution constante des menaces et des outils et contrôles créés pour y faire face, il n'est pas pratique de prescrire dans la norme la façon de protéger chaque *actif électronique* contre les maliciels. L'entité responsable détermine plutôt, pour chaque *système électronique BES*, quels *actifs électroniques* sont susceptibles de subir l'intrusion de maliciels, puis documente ses plans et processus de gestion de ces risques et fournit la preuve qu'elle suit ces plans et processus. Il existe de nombreuses options : solutions antivirus habituelles pour les systèmes d'exploitation courants, listes blanches, techniques d'isolement de réseau, solutions de détection et de prévention des intrusions, etc. Si une entité détient de nombreux *systèmes électroniques BES* ou *actifs électroniques* d'une architecture identique, elle peut établir un seul processus décrivant le mode de protection de tous les *actifs électroniques* semblables. Si un *actif électronique* particulier n'a pas de logiciel actualisable et que son code exécutable ne peut être modifié, cet *actif électronique* est considéré comme doté de sa propre méthode interne de protection contre les programmes malveillants.

3.2. Lorsqu'un programme malveillant est détecté sur un *actif électronique* dans le cadre de l'application de cette exigence, la menace posée par ce programme doit être atténuée. Dans les

situations où les programmes antivirus habituels sont utilisés, ceux-ci peuvent être configurés de manière à supprimer automatiquement ou à mettre en quarantaine les programmes malveillants. Dans les cas où des listes blanches sont utilisées, l'outil lui-même peut atténuer la menace en empêchant le programme de s'exécuter, mais d'autres mesures doivent être prises pour supprimer le programme malveillant de l'*actif électronique*. Dans certains cas, il est préférable, pour protéger la fiabilité, de ne pas supprimer ou mettre en quarantaine immédiatement le programme malveillant, par exemple si la disponibilité du système risque d'être compromise lorsque le programme malveillant est supprimé pendant que le système fonctionne et qu'il faut planifier une reconstruction du système. Il est alors possible d'accroître la surveillance et de prendre des mesures pour que le programme malveillant ne puisse communiquer avec d'autres systèmes. Dans d'autres cas, l'entité peut collaborer avec la police ou d'autres organisations gouvernementales pour surveiller étroitement le programme et dépister l'intrus. C'est pour ces raisons qu'il n'y a pas de délai maximal ou de méthode prescrite en vue de la suppression d'un programme malveillant ; l'exigence est plutôt d'atténuer la menace posée par le programme malveillant qui a été identifié.

Les entités doivent aussi être au courant des exigences de protection contre les maliciels applicables aux *actifs électroniques temporaires* et aux *supports de stockage amovibles* (« dispositifs temporaires ») énoncées dans la norme CIP-010-2. Les protections prescrites dans l'exigence E3 de la norme CIP-007-6 complètent ces obligations supplémentaires visant les dispositifs temporaires, mais ne suffisent pas pour s'y conformer.

3.3. Lorsque les technologies de détection de maliciels dépendent de signatures ou de séquences de code connues, leur efficacité pour protéger les systèmes contre des nouvelles menaces est liée à la capacité de tenir ces signatures et séquences à jour. L'entité doit disposer d'un processus documenté qui prévoit la vérification et l'installation des mises à jour des signatures ou des séquences de code. Dans un *système électronique BES*, certains *actifs électroniques* pourraient bénéficier de l'installation plus rapide des mises à jour, la disponibilité de ces actifs ne compromettant pas la disponibilité ou le fonctionnement du système électronique BES. Par exemple, certains postes de travail disposant d'une interface personne-machine faisant appel à des supports portatifs pourraient bénéficier des plus récentes mises à jour en tout temps, avec un minimum de vérification. Sur d'autres *actifs électroniques*, les mises à jour devraient être vérifiées intégralement avant la mise en œuvre, car un résultat « faux positif » pourrait nuire à la disponibilité du *système électronique BES*. La vérification ne doit pas avoir un impact négatif sur la fiabilité du BES. Elle doit être axée sur la mise à jour elle-même et sur le risque qu'elle nuise au *système électronique BES*. La vérification n'implique en aucun cas qu'une entité doive s'assurer qu'un maliciel est détecté s'il est introduit dans le système. Elle vise uniquement à faire en sorte que l'entité s'assure, avant d'installer une mise à jour, qu'elle n'aura pas d'incidence négative sur le *système électronique BES*.

Exigence E4

Consulter les publications NIST 800-92 et 800-137 pour des directives supplémentaires sur la surveillance des événements de sécurité.

4.1. Dans le contexte d'environnements informatiques complexes confrontés à des menaces et à des vulnérabilités qui ne cessent d'évoluer, il n'est pas pratique que la norme énumère tous les événements de sécurité justifiant une alerte ou une intervention en cas d'incident. L'entité responsable détermine plutôt quels événements informatiques doivent être journalisés et doivent faire l'objet d'alertes et d'un suivi compte tenu de son *système électronique BES* particulier.

Les événements de sécurité précis déjà visés par la version 4 des normes CIP sont reportés dans cette version. Ils comprennent les tentatives d'accès aux *points d'accès électroniques* qui auraient été répertoriées pour un *système électronique BES*, par exemple : i) tentatives bloquées d'accès au réseau, ii) tentatives d'accès d'utilisateurs distants, qu'elles aient réussi ou échoué, iii) tentatives bloquées d'accès au réseau à partir d'un VPN distant, et iv) tentatives réussies d'accès au réseau ou d'obtention d'information sur les flux dans le réseau.

Les événements associés aux accès et aux activités des utilisateurs sont notamment générés par les *actifs électroniques* situés à l'intérieur du *périmètre de sécurité électronique* et ayant la capacité de contrôler les accès. Ces types d'événement comprennent : i) l'authentification ayant réussi ou échoué, ii) la gestion des comptes, iii) l'accès aux objets, et iv) les processus entrepris et interrompus.

L'intention de la SDT n'est pas qu'une exception liée à la faisabilité technique (TFE) soit générée si un dispositif ne peut journaliser un événement en particulier. Son intention est plutôt que l'entité journalise tous les éléments de la liste à puces (fermeture de session par les utilisateurs, par exemple) que le dispositif est en mesure de journaliser. Si le dispositif n'a pas la capacité de journaliser un événement, l'entité demeure conforme.

4.2. Les alertes en temps réel permettent au système électronique de communiquer automatiquement des événements importants aux intervenants désignés. Cela nécessite la configuration d'un mécanisme de communication et l'établissement de règles d'analyse des journaux. Les alertes peuvent être configurées sous forme de courriels, de messages texte ou d'affichages et d'alarmes directement dans le système. Les règles d'analyse des journaux peuvent exister à l'intérieur du système d'exploitation, d'une application spécifique ou d'un système centralisé de surveillance des événements de sécurité. À un bout du spectre, une alerte en temps réel peut être un simple réglage sur une station terminale en cas d'échec d'ouverture de session et, à l'autre bout, un système de surveillance des événements de sécurité proposant de multiples options de communication d'alertes déclenchées par des règles complexes de corrélation des journaux.

Les événements déclencheurs d'alertes en temps réel peuvent être modifiés avec le temps à mesure que les administrateurs de système et les intervenants en cas d'incident apprennent à mieux reconnaître les types d'événements pouvant signaler un incident de cybersécurité. Il faut configurer les alertes en tenant compte de la nécessité de prévenir les intervenants quand un événement se produit, tout en évitant un accroissement indu du nombre des fausses alertes. La liste suivante comprend des exemples d'événements dont une entité responsable doit tenir compte lors de la configuration des alertes en temps réel :

- détection de maliciels ou d'activités malveillantes connus ou potentiels ;
- défaillance des mécanismes de journalisation des événements de sécurité ;
- échecs d'ouverture de session pour des comptes critiques ;
- ouverture de session interactive sur des comptes système ;
- activation de comptes ;
- utilisation de comptes nouvellement attribués ;
- tâches de gestion ou de modification de système effectuées par un utilisateur non autorisé ;
- tentatives d'authentification pour certains comptes en dehors des heures ouvrables ;
- changements de configuration non autorisés ;
- insertion d'un support de stockage amovible en infraction à une politique.

4.3 Les journaux créés conformément à l'alinéa 4.1 doivent être conservés dans les *actifs électroniques* ou les *systèmes électroniques BES* visés pendant au moins 90 jours. Cette période est différente de la période de conservation des pièces justificatives exigée dans les normes CIP afin de prouver la conformité historique d'une entité. Pour les fins d'audit, l'entité doit conserver une pièce justificative indiquant qu'elle a conservé les journaux portant sur 90 jours (par exemple, des preuves de l'élimination de journaux d'événements datant de plus de 90 jours avant la période de conservation des pièces justificatives).

4.4. L'examen des journaux au moins tous les 15 jours (environ toutes les deux semaines) peut consister dans l'analyse d'un résumé ou d'un échantillon d'événements journalisés. La publication spéciale SP800-92 du NIST contient beaucoup de conseils sur l'analyse périodique des journaux. Si un système centralisé de surveillance des événements de sécurité est employé, l'analyse des journaux peut être une analyse descendante commençant par un examen des tendances tirées des rapports sommaires. L'examen des journaux peut aussi être un prolongement de l'exercice consistant à repérer les événements nécessitant des alertes en temps réel selon lequel on analyserait les événements qui ne sont pas parfaitement compris ou qui pourraient provoquer d'innombrables alertes en temps réel.

Exigence E5

Les types de compte dont il est question dans cette exigence comprennent les suivants :

- Compte utilisateur partagé : compte employé par plusieurs utilisateurs – employés ou contractuels – dans le cours normal des activités. Il se trouve habituellement dans un dispositif qui ne prend pas en charge les comptes d'utilisateur individuel.
- Compte d'utilisateur individuel : compte employé par un seul utilisateur.
- Compte administratif : compte comportant des droits d'accès élargis permettant d'exécuter des fonctions administratives ou d'autres fonctions spécialisées. Le compte peut être individuel ou partagé.
- Compte système : compte utilisé pour exécuter des services sur un système (Web, DNS, courriel, etc.). Aucun utilisateur n'a accès à ce type de compte.

- Compte d'application : compte système particulier comportant des droits d'accès accordés au niveau de l'application, souvent utilisé pour accéder à une base de données.
- Compte d'invité : compte d'utilisateur individuel qui n'est pas habituellement utilisé par des employés ou des contractuels pour l'exécution de leurs tâches normales et qui n'est pas associé à un utilisateur particulier. Peut être partagé ou non par plusieurs utilisateurs.
- Compte d'accès distant : compte d'utilisateur individuel utilisé uniquement pour obtenir un accès distant interactif au *système électronique BES*.
- Compte générique : compte de groupe établi par le système d'exploitation ou par l'application pour la réalisation de certaines tâches. Diffère d'un compte utilisateur partagé en ce que les utilisateurs individuels ne reçoivent pas l'autorisation d'accéder à ce type de compte.

5.1 Voir la justification de l'exigence.

5.2 Dans la mesure du possible, les comptes par défaut et autres comptes génériques définis par un fournisseur doivent être retirés, renommés ou désactivés avant la mise en service de l'*actif électronique* ou du *système électronique BES*. Si ce n'est pas possible, les mots de passe par défaut doivent être changés. Tout compte par défaut ou autre compte générique qui demeure activé doit être documenté. Pour les configurations courantes, on peut procéder à cette documentation au niveau du *système électronique BES* ou à un niveau plus général.

5.3 Les entités peuvent choisir de désigner des personnes ayant accès aux comptes partagés par l'entremise du processus d'autorisation et de fourniture d'accès, auquel cas les registres d'autorisations individuelles suffisent pour assurer la conformité à cet alinéa de l'exigence. Les entités peuvent aussi choisir de tenir une liste distincte pour les comptes partagés. Les deux formes de preuves sont conformes au résultat visé, soit conserver le contrôle des comptes partagés.

5.4. Les mots de passe par défaut sont souvent publiés dans la documentation que les fournisseurs offrent à tous les clients utilisant ce type d'équipement et qu'ils diffusent parfois en ligne.

La possibilité de mots de passe exclusifs est précisée dans l'exigence pour les cas où l'*actif électronique* génère ou attribue des mots de passe par défaut pseudo-aléatoires au moment de la mise en service ou de l'installation. Il n'est alors pas nécessaire de changer le mot de passe par défaut parce que le système ou le fabricant l'a créé exclusivement pour l'*actif électronique*.

5.5. L'accès utilisateur interactif exclut l'accès à de l'information en lecture seule pour lequel la configuration de l'*actif électronique* ne peut être changée (afficheur intégré, rapports Web, etc.). Si un dispositif n'est pas en mesure d'assurer l'authentification, pour des raisons techniques ou opérationnelles, l'entité doit démontrer que tous les chemins d'accès utilisateur interactif distants et locaux sont configurés de manière à assurer l'authentification. La sécurité physique est suffisante comme configuration des accès locaux si elle est en mesure

d'enregistrer l'identité des personnes qui se trouvent dans le *périmètre de sécurité physique* à tout moment.

Des moyens techniques ou procéduraux sont requis pour imposer les paramètres de mot de passe lorsque le mot de passe est le seul justificatif d'authentification des personnes. Les moyens techniques s'appliquent aux *actifs électroniques* qui vérifient que le mot de passe choisi par une personne est conforme aux paramètres obligatoires avant de permettre l'authentification au moyen de ce mot de passe. Ils devraient être employés dans la plupart des cas où l'*actif électronique* le permet. Quant aux moyens procéduraux, il s'agit de procédures exigeant le respect des paramètres obligatoires ; ainsi, les personnes choisissant un mot de passe ont l'obligation de s'assurer qu'il est conforme aux paramètres obligatoires.

La complexité des mots de passe désigne la politique selon laquelle un *actif électronique* exige qu'un mot de passe comporte un ou plusieurs des types de caractères suivants : 1) lettres minuscules, 2) lettres majuscules, 3) caractères numériques et 4) caractères non alphanumériques ou spéciaux (#, \$, @, &, etc.), selon diverses combinaisons.

5.6 Des moyens techniques ou procéduraux sont requis pour imposer le changement de mot de passe lorsque le mot de passe est le seul justificatif d'authentification des personnes. Les moyens techniques s'appliquent aux *actifs électroniques* qui exigent le changement du mot de passe après une période donnée avant d'autoriser l'accès. Dans ce cas, il n'est pas nécessaire de changer le mot de passe avant la fin de cette période pourvu que l'*actif électronique* exige le changement du mot de passe après la première authentification réussie du compte au-delà de cette période. Les moyens procéduraux signifient le changement manuel des mots de passe servant à l'accès utilisateur interactif à une fréquence donnée.

5.7 Le blocage des comptes ou la génération d'alertes après un certain nombre d'échecs d'authentification sert à prévenir les accès non autorisés au moyen d'une attaque de craquage de mots de passe perpétrée en ligne. Le seuil du nombre d'échecs doit être assez élevé pour éviter les faux positifs imputables à des utilisateurs autorisés qui ne réussissent pas à s'authentifier, mais assez bas pour contrer les attaques étalées sur une longue période. Il peut être ajusté à l'environnement d'exploitation au fil du temps afin d'éviter les blocages de compte non nécessaires.

Les entités doivent faire attention, en configurant le blocage de comptes, d'éviter de bloquer les comptes nécessaires au *système électronique BES* pour une tâche assurant la fiabilité du BES. Dans un tel cas, il faut plutôt configurer la génération d'alertes en cas d'échec d'authentification.

Justification

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

Justification de l'exigence E1

Cette exigence vise à réduire au minimum la surface d'attaque des *systèmes électroniques BES* soit par la désactivation des ports d'entrée-sortie physiques et des services et ports logiques non nécessaires accessibles par le réseau, soit par une restriction de l'accès à ces ports et services.

En réponse au renvoi par la FERC (paragraphe 149 de son ordonnance 791) à la mesure de sécurité PE-4 de la norme NIST 800-53, révision 3, l'alinéa 1.2 a été modifié pour englober les *PCA* et les composants de communication non programmables. Cette extension de l'applicabilité étend la portée des dispositifs qui bénéficient de la « défense en profondeur » invoquée par l'alinéa 1.2 de l'exigence E1.

L'applicabilité est limitée aux composants de communication non programmables situés à la fois dans un *périmètre de sécurité physique* et dans un *périmètre de sécurité électronique* afin de permettre à l'entité responsable d'établir un *périmètre de sécurité électronique* étendu (avec des protections logiques correspondantes indiquées à l'alinéa 1.10 de l'exigence E1 et la norme CIP-006). Dans un tel scénario, les composants non programmables du réseau de communication peuvent se trouver hors du contrôle de l'entité responsable (s'ils font, par exemple, partie intégrante du réseau de télécommunication commercial).

Justification de l'exigence E2

La gestion des correctifs de sécurité est un moyen proactif utilisé pour faire le suivi des vulnérabilités connues en matière de sécurité et pour corriger celles-ci avant qu'elles ne puissent être exploitées de manière malveillante en vue de prendre le contrôle d'un *actif électronique BES* ou d'un *système électronique BES* ou de le rendre hors d'état de fonctionner.

Justification de l'exigence E3

La protection contre les programmes malveillants consiste à détecter et à limiter l'ajout de programmes malveillants aux *actifs électroniques* visés d'un *système électronique BES*. Ces programmes (virus, vers, réseaux de zombies, code ciblé tel que Stuxnet, etc.) peuvent compromettre la disponibilité ou l'intégrité d'un *système électronique BES*.

Justification de l'exigence E4

La surveillance des événements de sécurité a pour but la détection des accès non autorisés, des activités de reconnaissance et d'autres actes malveillants ciblant les *systèmes électroniques BES*. Elle comprend les activités liées à la constitution, au traitement et à la conservation des journaux de sécurité ainsi que les alertes. Ces journaux peuvent à la fois 1) permettre la détection d'un incident et 2) fournir une preuve utile à l'enquête sur un incident. La

conservation des journaux de sécurité est destinée à étayer l'analyse des données post-événement.

Cette exigence ne pénalise pas les échecs de journalisation ; elle précise plutôt les processus à mettre en place pour surveiller les échecs de journalisation et en aviser le personnel.

Justification de l'exigence E5

Il s'agit de faire en sorte qu'aucune personne autorisée ne puisse obtenir un accès électronique à un *système électronique BES* à moins d'être authentifiée, c'est-à-dire sans que ses renseignements d'authentification n'aient été validés. L'exigence E5 cherche aussi à réduire le risque que des mots de passe statiques utilisés comme facteur d'authentification soient compromis.

L'alinéa 5.1 de l'exigence vise à assurer que tout *système électronique BES* et tout *actif électronique* authentifie les personnes pouvant modifier l'information de configuration. Cette exigence porte notamment sur la configuration de l'authentification. L'autorisation des personnes est aussi abordée ailleurs dans les normes CIP sur la cybersécurité. L'accès utilisateur interactif exclut l'accès à de l'information en lecture seule pour lequel la configuration de l'*actif électronique* ne peut être changée (afficheur intégré, rapports Web, etc.). Si un dispositif n'est pas en mesure d'assurer l'authentification, pour des raisons techniques ou opérationnelles, l'entité doit démontrer que tous les chemins d'accès utilisateur interactif distants et locaux sont configurés de manière à assurer l'authentification. La sécurité physique est suffisante comme configuration des accès locaux si elle est en mesure d'enregistrer l'identité des personnes qui se trouvent dans le *périmètre de sécurité physique* à tout moment.

L'alinéa 5.2 de l'exigence porte sur les comptes par défaut et autres comptes génériques. Le fait que l'entité consigne quelle utilisation est faite des comptes par défaut et autres comptes génériques pouvant causer des vulnérabilités a l'avantage de faire en sorte qu'elle comprenne le risque éventuel représenté par ces comptes pour le *système électronique BES*. Cet alinéa de l'exigence évite de prescrire une intervention sur ces comptes parce que la solution la plus efficace dépend de chaque situation et que la suppression ou la désactivation du compte pourrait nuire à la fiabilité.

L'alinéa 5.3 de l'exigence porte sur les personnes ayant accès aux comptes partagés. L'objectif est de neutraliser le risque d'accès non autorisé par l'intermédiaire de comptes partagés. Cette exigence est différente de celles d'autres normes CIP sur la cybersécurité visant l'autorisation de l'accès. Une entité peut autoriser l'accès sans savoir qui a accès à un compte partagé. L'entité qui n'aurait pas la liste des personnes ayant accès aux comptes partagés pourrait difficilement retirer ces droits d'accès à quiconque n'en a plus besoin. Le terme « autorisé » est employé dans l'exigence pour préciser que le fait qu'une personne enregistre ou perde un mot de passe ou qu'elle le partage sans autorisation ne constitue pas une non-conformité en vertu de cette exigence.

L'alinéa 5.4 de l'exigence porte sur les mots de passe par défaut. Leur modification élimine une vulnérabilité facilement exploitable de nombreux systèmes et applications. Les mots de passe

pseudo-aléatoires générés automatiquement ne sont pas considérés comme des mots de passe par défaut.

En ce qui concerne l'authentification des utilisateurs par mot de passe, l'utilisation de mots de passe forts et leur modification périodique contribuent à atténuer le risque de réussite des attaques de craquage de mots de passe ainsi que le risque de divulgation accidentelle de mots de passe à des personnes non autorisées. L'équipe de rédaction a envisagé plusieurs approches afin de rendre cette exigence assez efficace et flexible pour permettre aux entités responsables de prendre les bonnes décisions en matière de sécurité. L'une des approches envisagées consistait à exiger une entropie minimale pour les mots de passe ; or, le calcul de la véritable entropie d'information est beaucoup plus complexe et se fonde sur plusieurs hypothèses concernant le choix de mots de passe par les utilisateurs. Ces derniers peuvent choisir des mots de passe faibles dont l'entropie est nettement inférieure au minimum calculé.

L'équipe de rédaction a aussi choisi de ne pas exiger d'exceptions liées à la faisabilité technique pour les dispositifs qui ne respectent pas les paramètres de longueur et de complexité des mots de passe. L'objectif de cette exigence est d'appliquer une politique de mot de passe mesurable afin de prévenir les tentatives de craquage ; le remplacement de dispositifs simplement pour respecter une politique précise sur les mots de passe n'atteint pas cet objectif. Cependant, l'exigence a été renforcée de manière à exiger le verrouillage de comptes ou la génération d'alertes en cas d'échec d'ouverture de session, ce qui permet généralement de mieux atteindre l'objectif visé.

L'exigence de changement des mots de passe permet de contrer la situation où une tentative de craquage aurait réussi à dévoiler un mot de passe crypté, ainsi que de remplacer tout mot de passe qui aurait été divulgué accidentellement au fil du temps. L'exigence donne à l'entité le loisir de préciser quelle fréquence de changement des mots de passe permet d'atteindre l'objectif. En particulier, l'équipe de rédaction a jugé plus efficace que la fréquence soit déterminée en fonction de plusieurs facteurs plutôt que d'être fixée pour tous les *systèmes électroniques BES* visés par la norme. En général, les mots de passe servant à l'authentification des utilisateurs doivent être changés au moins une fois par année. Cette fréquence peut parfois être réduite : ainsi, des mots de passe d'applications longs et pseudo-aléatoires pourraient être changés très peu fréquemment. Par ailleurs, les mots de passe employés uniquement comme méthode d'authentification faible d'une application (par exemple, l'accès à la configuration d'un relais) pourraient n'être changés que dans le cadre de l'entretien de routine.

L'*actif électronique* doit appliquer automatiquement la politique sur les mots de passe aux comptes d'utilisateur individuel. Toutefois, dans le cas des comptes partagés pour lesquels il n'existe aucun mécanisme d'application de la politique sur les mots de passe, l'entité responsable peut recourir à des procédures ainsi qu'à une évaluation interne et à un audit.

L'alinéa 5.7 de l'exigence aide à prévenir les attaques perpétrées en ligne visant les mots de passe en limitant le nombre de tentatives possibles. Il s'agit soit de limiter le nombre de tentatives d'authentification, soit de générer une alerte après un certain nombre d'échecs. Les entités doivent user de prudence avant de limiter le nombre de tentatives d'authentification

pour tous les comptes, car cela peut ouvrir la possibilité d'une attaque par déni de service visant le *système électronique BES*.

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 — Gestion de la sécurité des systèmes
2. **Numéro :** CIP-007-6
3. **Objet :** Aucune disposition particulière
4. **Applicabilité :**

4.1. Entités fonctionnelles

Aucune disposition particulière

4.2. Installations

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

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

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

5. Date d'entrée en vigueur au Québec :

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

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

Norme	Entité	Dates d'implantation aux États-Unis	Date d'entrée en vigueur proposée au Québec		Justification
			Impacts moyen et élevé	Impacts faible	
<ul style="list-style-type: none"> CIP-007-6 	Entités visées par la version 1 des normes CIP adoptées par la Régie.	2016-07-01	2017-07-01	2017-07-01	Uniformisation des pratiques avec les autres juridictions.
	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes.		2018-10-01	2019-10-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
	Entités qui possèdent des installations de production à vocation industrielle		2019-04-01	2020-04-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.

Norme	Entité	Dates d'implantation aux États-Unis	Date d'entrée en vigueur proposée au Québec		Justification
			Impacts moyen et élevé	Impacts faible	
<ul style="list-style-type: none"> CIP-007-6, E1, l'alinéa 1.2 (pour les PCA et les composantes de communication non programmables situés à la fois dans un périmètre de sécurité physique et dans un périmètre de sécurité électronique pour les systèmes électroniques BES à impact moyen ou élevé) 	Entités visées par la version 1 des normes CIP adoptées par la Régie.	2017-04-01	2017-07-01	2018-07-01	Uniformisation des pratiques avec les autres juridictions.
	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes.		2018-10-01	2019-10-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
	Entités qui possèdent des installations de production à vocation industrielle		2019-04-01	2020-04-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.

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

6. Contexte :

Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et de mise en application des normes

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Justification

Aucune disposition particulière

Historique des versions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe.	Nouvelle