

A. Introduction

1. **Titre :** Cybersécurité — Protection de l'information
2. **Numéro :** CIP-011-1
3. **Objet :** Empêcher tout accès non autorisé à l'information de *système électronique BES* en définissant des exigences de protection de l'information visant à prévenir toute compromission pouvant entraîner un fonctionnement incorrect ou une instabilité dans le 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* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou 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 humain.
 - 4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.
 - 4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou 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 groupes de production suivants à démarrer.
 - 4.1.3 **Exploitant d'installation de production**
 - 4.1.4 **Propriétaire d'installation de production**

4.1.5 Coordonnateur 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* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

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

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou 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 groupes de production suivants à démarrer.

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-011-1 :

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 à la norme CFR 10, section 73.54 ;
- 4.2.3.4** dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;
- 4.2.3.5** les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates de mise en vigueur

1. **24 mois minimum** – La norme CIP-011-1 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-011-1 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

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

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui correspondent à toutes les parties d'exigence 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.

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à habilitier l'industrie à identifier, à évaluer et à corriger les lacunes dans la mise en œuvre de certaines exigences. L'intention est de changer la manière

de considérer les infractions dans ces exigences, de sorte qu'il ne s'agisse plus de savoir *si* une lacune existe, mais plutôt d'identifier, d'évaluer et de corriger les lacunes. Ceci est présenté dans ces exigences en modifiant la notion de « mise en œuvre » de la façon suivante :

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

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes. Les processus documentés eux-mêmes n'ont pas à intégrer la démarche « détecter, évaluer et corriger les lacunes » décrite au paragraphe précédent, car cette démarche est liée à la manière de mettre en œuvre les processus documentés et pourrait être réalisée par d'autres mesures de contrôle ou de gestion de la conformité.

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

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

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

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

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

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

Colonnes « Systèmes visés » des tableaux :

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

- **Systèmes électroniques BES à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS)** – Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification, et systèmes de surveillance de registre d'événement et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès 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, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs programmes documentés de protection de l'information qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-011-1) – Protection de l'information. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*
- M1.** Les pièces justificatives attestant du programme de protection de l'information doivent comprendre toutes les parties d'exigence applicables du tableau E1 (CIP-011-1) – Protection de l'information, et des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

| Tableau E1 (CIP-011-1) – Protection de l'information | | | |
|--|---|---|--|
| Partie | Systèmes visés | Exigences | Mesures |
| 1.1 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; et 2. PACS associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; et 2. PACS associés. | Méthode(s) permettant d'identifier l'information qui répond à la définition d' <i>information de système électronique BES</i> . | <p>Exemples non limitatifs de pièces justificatives acceptables :</p> <ul style="list-style-type: none"> • méthode documentée permettant d'identifier l'<i>information de système électronique BES</i> à partir du programme de protection de l'information de l'entité ; ou • indications sur l'information (étiquetage, classification, etc.) qui identifie l'<i>information de système électronique BES</i> telle que désignée dans le programme de protection de l'information de l'entité ; ou • matériel de formation qui donne au personnel des connaissances suffisantes pour reconnaître l'<i>information de système électronique BES</i> ; ou • archive ou emplacement électronique et physique affecté au stockage de l'<i>information de système électronique BES</i> dans le cadre du programme de protection de l'information de l'entité. |

| Tableau E1 (CIP-011-1) – Protection de l'information | | | |
|--|---|---|--|
| Partie | Systèmes visés | Exigences | Mesures |
| 1.2 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; et 2. PACS associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; et 2. PACS associés. | Procédure(s) pour la protection et la manipulation sécuritaire de <i>l'information de système électronique BES</i> , y compris pour le stockage, le transport et l'utilisation. | <p>Exemples non limitatifs de pièces justificatives acceptables :</p> <ul style="list-style-type: none"> • procédures pour la protection et la manipulation sécuritaire de <i>l'information de système électronique BES</i>, portant sur des aspects comme le stockage, la sécurité pendant le transport et l'utilisation ; ou • documents indiquant que <i>l'information de système électronique BES</i> est manipulée conformément aux procédures documentées de l'entité. |

- E2.** Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-011-1) – Réutilisation et élimination des *actifs électroniques BES*.
[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]
- M2.** Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-011-1) – Réutilisation et élimination des *actifs électroniques BES*, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

| Tableau E2 (CIP-011-1) – Réutilisation et élimination des actifs électroniques BES | | | |
|--|---|--|--|
| Partie | Systèmes visés | Exigences | Mesures |
| 2.1 | <p><i>Systèmes électroniques BES</i> à impact élevé et leurs :</p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES</i> à impact moyen et leurs :</p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | <p>Avant d'autoriser la réutilisation d'un <i>actif électronique</i> visé qui contient de l'<i>information de système électronique BES</i> (sauf si cet actif est réutilisé dans d'autres systèmes indiqués à la colonne Systèmes visés), l'entité responsable doit faire en sorte d'empêcher toute récupération non autorisée d'<i>information de système électronique BES</i> du support d'information de l'<i>actif électronique</i> en question.</p> | <p>Exemples non limitatifs de pièces justificatives acceptables :</p> <ul style="list-style-type: none"> • documents de suivi des mesures d'expurgation visant à empêcher toute récupération non autorisée d'<i>information de système électronique BES</i>, notamment par écrasement, purge ou destruction ; ou • documents de suivi de mesures comme le cryptage, la rétention dans le <i>périmètre de sécurité physique</i> ou d'autres moyens d'empêcher la récupération non autorisée d'<i>information de système électronique BES</i>. |

Tableau E2 (CIP-011-1) – Réutilisation et élimination des actifs électroniques BES

| Partie | Systèmes visés | Exigences | Mesures |
|--------|---|---|---|
| 2.2 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | <p>Avant l'élimination d'un <i>actif électronique</i> visé qui contient de l'<i>information de système électronique BES</i>, l'entité responsable doit faire en sorte d'empêcher toute récupération non autorisée d'<i>information de système électronique BES</i> de l'<i>actif électronique</i> en question, ou encore de détruire son support d'information.</p> | <p>Exemples non limitatifs de pièces justificatives acceptables :</p> <ul style="list-style-type: none"> • documents attestant que le support d'information a été détruit avant l'élimination d'un <i>actif électronique</i> visé ; ou • documents attestant les mesures prises pour empêcher la récupération non autorisée d'<i>information de système électronique BES</i> d'un <i>actif électronique</i> visé avant son élimination. |

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l'application des normes

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

1.2. Conservation des pièces justificatives

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

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête :

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

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

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité

- Aucune

2. Tableau des éléments de conformité

| E# | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-011-1) | | | |
|----|---------------------------------|-------|---|------------|--|---|
| | | | VSL Faible | VSL Modéré | VSL Élevé | VSL Critique |
| E1 | Planification de l'exploitation | Moyen | Sans objet | | <p>L'entité responsable a mis en œuvre un programme de protection de l'information de système électronique BES qui comprend une ou plusieurs méthodes pour identifier l'information de système électronique BES et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (1.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un programme de protection de l'information de système électronique BES qui comprend une ou plusieurs méthodes pour identifier</p> | <p>L'entité responsable n'a pas documenté ou mis en œuvre un programme de protection de l'information de système électronique BES. (E1)</p> |

| E# | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-011-1) | | | |
|----|---------|-----|---|------------|--|--------------|
| | | | VSL Faible | VSL Modéré | VSL Élevé | VSL Critique |
| | | | | | <p><i>l'information de système électronique BES, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.1)</i></p> <p>OU</p> <p>L'entité responsable a mis en œuvre un programme de protection de <i>l'information de système électronique BES</i> qui comprend une ou plusieurs procédures pour la protection et la manipulation sécuritaire de <i>l'information de système électronique BES</i> et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (1.2)</p> <p>OU</p> | |

| E# | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-011-1) | | | |
|----|---------------------------------|--------|---|---|--|---|
| | | | VSL Faible | VSL Modéré | VSL Élevé | VSL Critique |
| | | | | | L'entité responsable a mis en œuvre un programme de protection de l'information de système électronique BES qui comprend une ou plusieurs procédures pour la protection et la manipulation sécuritaire de l'information de système électronique BES, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.2) | |
| E2 | Planification de l'exploitation | Faible | Sans objet | L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais n'a pas inclus de processus de réutilisation visant à empêcher la récupération non autorisée | L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais n'a pas inclus de processus de disposition ou de destruction de support afin d'empêcher la récupération non | L'entité responsable n'a pas documenté ou mis en œuvre aucun processus pour les parties d'exigence applicables du Tableau E2 (CIP 011 1) – Réutilisation et élimination des <i>actifs</i> |

| E# | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-011-1) | | | |
|----|---------|-----|---|--|--|--------------------------------|
| | | | VSL Faible | VSL Modéré | VSL Élevé | VSL Critique |
| | | | | <i>d'information de système électronique BES à partir de l'actif électronique BES. (2.1)</i> | <i>autorisée d'information de système électronique BES à partir de l'actif électronique BES. (2.2)</i> | <i>électroniques BES. (E2)</i> |

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Principes directeurs et fondements techniques

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

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

La section « 4.1. Entités fonctionnelles » est la liste des entités fonctionnelles de la NERC auxquelles s'applique la norme. Si l'entité est enregistrée au titre d'une ou de plusieurs des entités fonctionnelles énumérées à la section 4.1, alors les normes CIP sur la cybersécurité de la NERC s'appliquent. Il est à noter qu'il y a une restriction à la section 4.1 qui limite l'applicabilité dans le cas des distributeurs à ceux qui détiennent certains types de systèmes et d'équipements énumérés à la section 4.2.

La section « 4.2. Installations » définit la portée des installations, systèmes et équipements détenus par l'entité responsable qualifiée à la section 4.1, qui est visée par les exigences de la norme. Tel qu'indiqué à la section exemption 4.2.3.5, cette norme ne s'applique pas aux entités responsables qui n'ont pas de systèmes électroniques BES à impact élevé ou à impact moyen selon la catégorisation de la CIP-002- 5. Outre l'ensemble des installations du BES, des centres de contrôle et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements détenus par les distributeurs. Bien que le terme « installations » du glossaire de la NERC comprenne déjà la caractéristique BES, l'utilisation additionnelle du terme « BES » vise ici à renforcer la portée d'applicabilité pour ces installations, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les installations, systèmes et équipements visés par les normes.

Exigence E1 :

Les entités responsables sont libres d'utiliser les systèmes existants de gestion des changements et des actifs. Cependant, l'information que contiennent ces systèmes doit être évaluée, car les exigences de protection de l'information s'appliquent toujours.

La justification de cette exigence est déjà présente dans les versions précédentes des normes CIP, ainsi que dans l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe.

Cette exigence stipule qu'il faut désigner l'*information de système électronique BES*. L'entité responsable dispose d'une certaine latitude quant à la mise en œuvre de cette exigence. L'entité responsable devrait expliquer par quels moyens l'*information de système électronique BES* est désignée dans son programme de protection de l'information. Par exemple, l'entité peut décider de marquer ou d'étiqueter les documents. Il n'est pas exigé d'établir des classes distinctes d'*information de système électronique BES*. Cependant, l'entité responsable est libre de le faire si elle le souhaite. Pour autant que le programme de protection de l'information englobe tous les éléments pertinents, l'entité peut aller plus loin et créer des niveaux de classification (public, confidentiel, usage interne, etc.). Si l'entité responsable choisit d'utiliser

un système de classification, elle doit documenter les classes de ce système et tout étiquetage connexe dans son programme d'*information de système électronique BES*.

L'entité responsable peut stocker toute l'information concernant les *systèmes électroniques BES* dans une archive ou un emplacement séparé (physique ou électronique) protégé par un contrôle d'accès. Par exemple, le programme de l'entité responsable pourrait spécifier que toute l'information stockée dans une archive particulière est une *information de système électronique BES*, ou que toute l'information stockée dans telle section d'une archive particulière est une *information de système électronique BES*, ou encore que toutes les copies papier de cette information sont stockées dans une partie sécurisée du bâtiment. D'autres méthodes pour la mise en œuvre de cette exigence sont suggérées à la section Mesures. Cependant, ces méthodes ne forment pas une liste exhaustive, et l'entité responsable peut recourir à d'autres moyens pour désigner l'*information de système électronique BES*.

Le SDT souhaite préciser que cette exigence ne s'applique pas à l'information accessible au public, comme les manuels de fournisseurs consultables sur des sites Web publics, non plus qu'à toute information considérée comme divulgable au grand public.

La protection de l'information englobe les versions électronique et papier. L'exigence E1.2 prescrit une ou plusieurs procédures pour la protection et la manipulation sécuritaire de l'*information de système électronique BES*, notamment le stockage, le transport et l'utilisation.

Le programme écrit de protection de l'information de l'entité doit expliquer comment celle-ci gère divers aspects de la protection de l'*information de système électronique BES*, notamment pendant le transport, afin de prévenir tout accès non autorisé, toute mauvaise utilisation ou toute corruption, et aussi pour protéger la confidentialité de l'information transmise. Par exemple, le recours à un fournisseur de service de télécommunications tiers plutôt qu'à une infrastructure détenue par l'organisation peut justifier le cryptage de l'information. L'entité peut choisir d'établir un trajet de communication de confiance pour le transport de l'*information de système électronique BES* ; ce trajet de confiance utiliserait un mécanisme d'authentification ou d'autres mesures pour assurer la sécurité pendant le transport. L'entité peut adopter d'autres mesures de protection physique, comme le transport par messenger ou l'utilisation d'un contenant de transport verrouillé. La présente norme ne cherche pas à imposer un moyen particulier de sécuriser l'information pendant son transport.

Un bon programme de protection de l'information spécifie par écrit les circonstances dans lesquelles l'*information de système électronique BES* peut être partagée avec des tiers ou être utilisée par ceux-ci. L'entité ne doit diffuser ou partager l'information que selon le principe de l'accès sélectif. Par exemple, l'entité peut spécifier qu'un accord de confidentialité, une entente de non-divulgence, un contrat ou toute autre convention écrite concernant l'utilisation de l'information doit être en place entre l'entité et le tiers. Le programme de protection de l'information de l'entité doit spécifier les modalités de partage de l'*information de système électronique BES* avec des tiers ou de son utilisation par ceux-ci, par exemple une entente de non-divulgence. L'entité doit ensuite respecter son programme documenté. Ces exigences n'imposent pas un type particulier d'arrangement.

Exigence E2 :

Cette exigence permet le retrait du service des *systèmes électroniques BES* et leur analyse avec leur support intact, car cela ne constitue pas une autorisation de réutilisation. Cependant, si après analyse le support doit être réutilisé à l'extérieur d'un *système électronique BES* ou doit être éliminé, l'entité doit prendre des mesures pour empêcher la récupération non autorisée de l'*information de système électronique BES* présente sur le support.

La justification de cette exigence est déjà présente dans les versions précédentes des normes CIP, ainsi que dans l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe.

Si un *actif électronique* visé est retiré du périmètre de sécurité physique avant que des mesures aient été prises pour empêcher la récupération non autorisée de l'*information de système électronique BES* ou avant que le support d'information ait été détruit, l'entité responsable doit tenir un dossier indiquant le détenteur du support d'information pendant que ce dernier se trouve hors du *périmètre de sécurité physique* avant l'application par l'entité des mesures prescrites à l'exigence E2.

On appelle « expurgation » le procédé qui consiste à éliminer l'information d'un support de données de manière à assurer raisonnablement que l'information ne pourra pas être récupérée ou reconstituée. Les moyens d'expurgation sont généralement divisés en quatre catégories : la mise au rebut, l'écrasement, la purge et la destruction. Aux fins de la présente exigence, la mise au rebut en elle-même – sauf dans certaines circonstances spéciales, comme le recours à un cryptage fort pour un disque utilisé dans un réseau de stockage (SAN) ou un autre support – ne doit jamais être jugée acceptable. Les techniques d'écrasement peuvent constituer un moyen d'expurgation adéquat pour les supports destinés à être réutilisés, tandis que les techniques de purge peuvent mieux convenir pour les supports destinés à l'élimination.

L'information suivante, tirée de la publication spéciale 800-88 du NIST, donne des précisions supplémentaires sur les types de mesures que l'entité pourrait prendre pour empêcher la récupération non autorisée de l'*information de système électronique BES* à partir de ses supports d'information :

Écrasement : Cette méthode d'expurgation consiste à écrire des données non sensibles à la place des données existantes du support, au moyen d'un logiciel ou d'un appareil spécial. Ce procédé peut écraser ainsi non seulement l'emplacement logique du ou des fichiers en cause (par exemple, la table d'allocation de fichiers), mais aussi tous les emplacements mémoire adressables. Cette opération a pour objet de remplacer les données existantes par des données quelconques. L'écrasement n'est pas possible dans le cas d'un support endommagé ou non réinscriptible. Le type et la taille du support peuvent aussi déterminer si l'écrasement est une méthode d'expurgation convenable [800-36].

Purge : La démagnétisation et l'exécution de la commande d'effacement sécurisé du microprogramme (pour les disques ATA seulement) sont des méthodes de purge

acceptables. La démagnétisation consiste à exposer le support magnétique à un fort champ magnétique afin de perturber les domaines magnétiques d'enregistrement ; ce champ magnétique est produit par un démagnétiseur. Il existe différents types de démagnétiseur (à faible puissance, à grande puissance, etc.) selon le type de support magnétique qu'ils peuvent traiter. Les démagnétiseurs comportent un aimant permanent puissant ou une bobine électromagnétique. La démagnétisation convient particulièrement pour purger un support endommagé, inopérant ou de très grande capacité, ou pour effacer rapidement des disquettes. [800-36]

La commande d'effacement sécurisé (disques ATA) et la démagnétisation sont des exemples de méthodes de purge acceptables. La démagnétisation d'un disque dur détruit habituellement celui-ci, car elle efface aussi le microprogramme qui commande le disque.

Destruction : Il existe de nombreux moyens pour détruire un support d'information. La désintégration, la pulvérisation, la fusion et l'incinération sont des procédés d'expurgation conçus pour détruire complètement le support. On les confie généralement à une entreprise agréée de destruction de produits métalliques ou d'incinération disposant des moyens techniques appropriés pour effectuer cette opération de manière efficace, sécurisée et sécuritaire. Les supports optiques, notamment les cédéroms (réinscriptibles ou non), les disques optiques (DVD) et les disques magnéto-optiques, doivent être détruits par pulvérisation, par déchiquetage transversal ou par combustion.

Dans certains cas, notamment pour de l'équipement réseau, il peut être nécessaire de consulter le fabricant pour connaître la méthode d'expurgation appropriée.

Il est de la plus grande importance que l'organisation tienne un dossier de ses activités d'expurgation afin d'empêcher la récupération non autorisée d'*information de système électronique BES*. Les entités sont fortement invitées à consulter la publication spéciale 800-88 du NIST pour de plus amples renseignements sur l'élaboration de procédés d'expurgation des supports.

Raisonnement :

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

Raisonnement pour E1 :

L'exigence d'un programme de protection de l'information vise à empêcher tout accès non autorisé à l'*information de système électronique BES*.

Sommaire des modifications : Les exigences E4, E4.2 et E4.3 de la norme CIP 003 4 ont été transférées à l'exigence E1 de la norme CIP 011. L'exigence E4.1 de la norme CIP 003 4 a été transférée à la définition du terme « information de système électronique BES ».

Référence à une version précédente : (Partie 1.1) CIP-003-3, E4 ; CIP-003-3, E4.2

Justification des modifications : (Partie 1.1)

Le SDT a éliminé l'exigence explicite de classification, car il n'est pas nécessaire d'avoir plusieurs niveaux de protection (public, confidentiel, usage interne, etc.). Cette modification n'interdit pas pour autant les niveaux de classification, ce qui offre une plus grande souplesse pour l'intégration par l'entité du programme CIP de protection de l'information à ses activités normales.

Référence à une version précédente : (Partie 1.2) CIP-003-3, E4

Justification des modifications : (Partie 1.2)

Le SDT a remplacé la formulation « protéger les informations » par « procédures visant la protection et la manipulation sécuritaire de l'information » afin de préciser la protection requise.

Raisonnement pour E2 :

Le processus de réutilisation et d'élimination des *actifs électroniques BES* vise à empêcher toute diffusion non autorisée d'*information de système électronique BES* en cas de réutilisation ou d'élimination de ces actifs.

Référence à une version précédente : (Partie 2.1) CIP-007-3, E7.2

Justification des modifications : (Partie 2.1)

Conformément à l'ordonnance 706 de la FERC, paragraphe 631, le SDT précise qu'il s'agit d'empêcher toute récupération non autorisée d'information à partir du support. Le mot « effacer » n'est plus utilisé puisque, selon le support utilisé, l'effacement peut ne pas être un moyen suffisant pour atteindre le but visé.

Référence à une version précédente : (Partie 2.2) CIP-007-3, E7.1

Justification des modifications : (Partie 2.2)

Conformément à l'ordonnance 706 de la FERC, paragraphe 631, le SDT précise qu'il s'agit d'empêcher toute récupération non autorisée d'information à partir du support. Le mot « effacer » n'est plus utilisé puisque, selon le support utilisé, l'effacement peut ne pas être un moyen suffisant pour atteindre le but visé.

Le SDT a aussi éliminé l'exigence concernant la tenue de registres de retrait ou de redéploiement, de tels registres étant considérés comme une mesure d'attestation de l'exigence en vigueur, et non comme une exigence à proprement parler.

Historique des versions

| Version | Date | Intervention | Suivi des modifications |
|---------|------------------|---|--|
| 1 | 26 novembre 2012 | Adoption par le conseil d'administration de la NERC | Cette norme définit les exigences de protection de l'information en coordination avec d'autres normes CIP et met en œuvre certaines dispositions de l'ordonnance 706 de la FERC. |
| 1 | 22 novembre 2013 | Émission d'une ordonnance de la FERC approuvant CIP-010-1 (L'ordonnance entre en vigueur le 3 février 2014) | |

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 — Protection de l'information

2. **Numéro :** CIP-011-1

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

Installations

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

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 : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

1.1. **Responsable de la surveillance de l'application des normes**

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

1.2. **Conservation des pièces justificatives**

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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