« *Implementation Guidance* » (Guide d'application) de la norme CIP-004-7 (version française)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VERSION PRÉLIMINAIRE

Cybersécurité – Personnel et formation

Guide d'application de la norme de fiabilité CIP-004-7

Mars 2021

FIABILITÉ | RÉSILIENCE | SÉCURITÉ




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table des matières

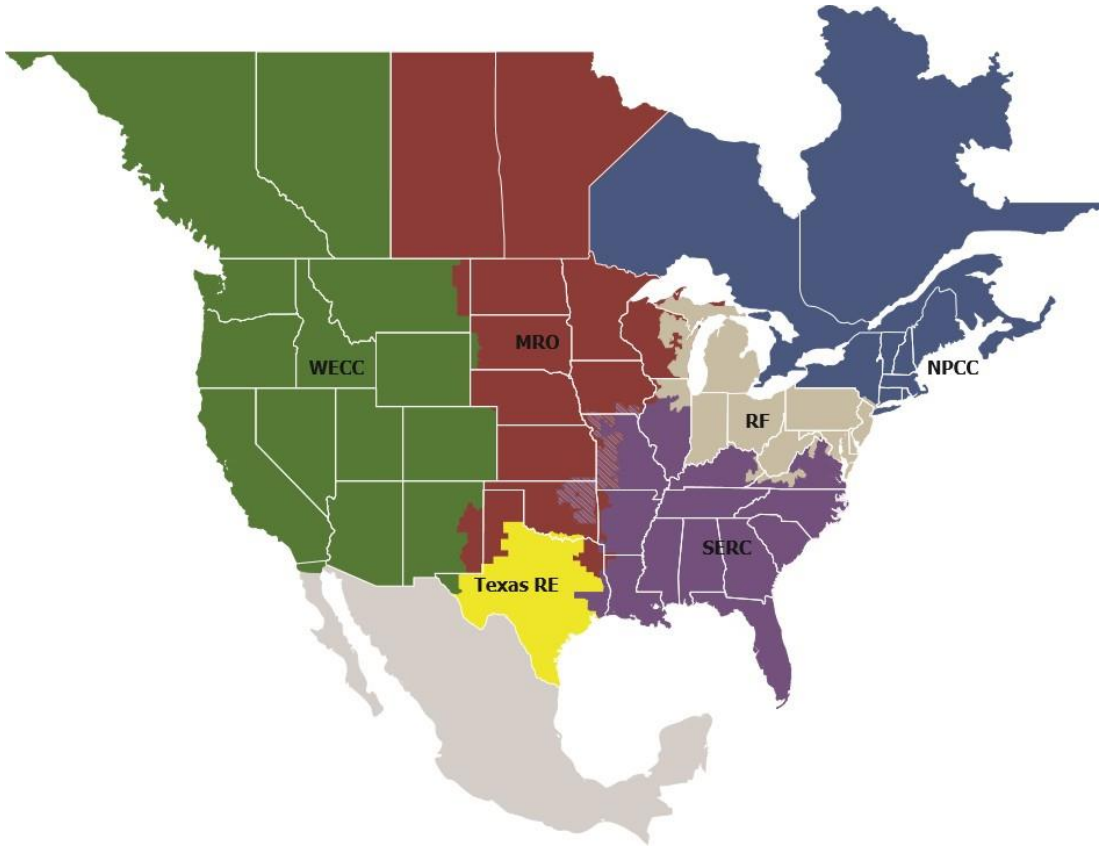
Préface

L'électricité est un élément essentiel du tissu de nos sociétés modernes, et l'organisme de fiabilité électrique (ERO) a pour mission de renforcer ce tissu. L'ERO, qui regroupe la North American Electric Reliability Corporation (NERC) et les six entités régionales, veille à maximiser la fiabilité et la sécurité du *système électrique interconnecté* (*BPS*) de l'Amérique du Nord. Nous travaillons en permanence à réduire de manière efficace et efficiente les risques pour la fiabilité et la sécurité du réseau électrique.

Fiabilité | Résilience | Sécurité

Parce que près de 400 millions de citoyens en Amérique du Nord comptent sur nous

Le *système électrique interconnecté* de l'Amérique du Nord est divisé en six territoires d'entités régionales, comme le montrent la carte et le tableau ci-dessous. Les zones combinant deux couleurs indiquent des chevauchements, car certains *responsables de l'approvisionnement* sont actifs dans une région alors que les *propriétaires d'installation de transport* et les *exploitants de réseau de transport* associés sont actifs dans une autre région.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst Corporation
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Ce Guide d'application a été préparé afin de présenter des exemples de démarches de conformité avec la norme CIP-004-7. Ce guide n'impose pas une démarche unique, mais indique différentes démarches qui permettront de réaliser la conformité avec la norme. Il ne s'agit d'ailleurs que d'exemples, et les entités sont donc libres de choisir toute autre démarche plus adaptée à leur situation particulière[1]. Le présent document, *Guide d'application de la norme de fiabilité CIP-004-7*, n'est pas une *norme de fiabilité* et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

Les entités responsables pourront compléter utilement la lecture du présent Guide d'application en consultant l'information présentée par l'équipe de rédaction dans le document *Justification technique de la norme de fiabilité CIP-004-7*.

1. Politique de la NERC relative aux lignes directrices sur la conformité.

Exigence E1

Remarques générales sur l'exigence E1

Aucune

Directives d'application pour l'exigence E1

Aucune

Exigence E2

Remarques générales sur l'exigence E2

Aucune

Directives d'application pour l'exigence E2

L'entité responsable a la liberté de définir son propre programme de formation, qui peut comprendre plusieurs modules et modes de prestation, mais un seul programme de formation pour toutes les personnes à former est aussi acceptable. L'entité responsable peut, à sa guise, axer la formation sur les fonctions, les rôles ou les responsabilités.

Exigence E3

Remarques générales sur l'exigence E3

Aucune

Directives d'application pour l'exigence E3

Aucune

Exigence E4

Remarques générales sur l'exigence E4

Aucune

Directives d'application pour l'exigence E4

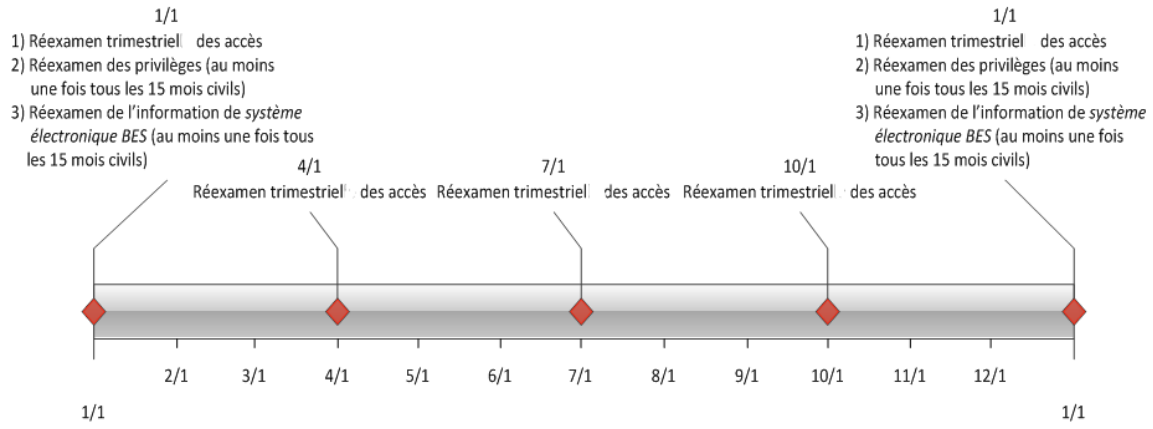
Envisager d'inclure la ou les personnes habilitées par l'entité responsable à autoriser les accès dans les délégations indiquées à la norme CIP-003-8.

Pour assurer une séparation adéquate des tâches, l'autorisation et la fourniture d'accès ne doivent pas être assumées par la même personne dans la mesure du possible. La séparation des tâches doit être prise en compte au moment de la réalisation des réexamens selon l'exigence E4. La personne chargée du réexamen ne doit pas être celle qui fournit les accès.

Les réexamens trimestriels peuvent consister à comparer la liste des personnes auxquelles un accès a réellement été fourni avec le registre des personnes pour lesquelles la fourniture d'un accès a été autorisée. La liste des personnes auxquelles un accès a été fourni peut être une liste de comptes générée automatiquement. Toutefois, dans un *système électronique BES* comptant plusieurs bases de données de comptes, la liste des personnes auxquelles un accès a été fourni peut provenir d'autres sources, comme des activités de fourniture d'accès ou une base de données de comptes utilisateurs qui sert habituellement de point de départ à la fourniture des accès.

Les entités peuvent optimiser le réexamen aux 15 mois civils en mettant en place un accès basé sur les rôles. Cette méthode consiste à définir les rôles au sein du système (répartiteur, technicien, récepteur de rapports, administrateur, etc.), puis à grouper les droits d'accès selon ces différents rôles, et enfin à assigner leurs rôles aux utilisateurs. Ce système ne suppose aucun logiciel particulier et on peut le mettre en place en définissant des processus de fourniture d'accès particuliers pour chaque rôle ne permettant pas l'affectation de groupes d'accès.

Un calendrier type de tous les réexamens énoncés aux exigences E4 et E6 est illustré ci-dessous.



Exigence E5

Remarques générales sur l'exigence E5

Aucune

Directives d'application pour l'exigence E5

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

Scénario	Processus possible
Départ involontaire immédiat	Un représentant des ressources humaines ou un agent de sécurité accompagne la personne hors du lieu de travail et le superviseur de celle-ci ou le personnel des ressources humaines demande au personnel compétent d'entamer le processus de révocation.
Départ involontaire prévu	Le personnel des ressources humaines est avisé du départ et collabore avec le personnel compétent pour que l'accès soit révoqué au moment du départ.
Départ volontaire	Le personnel des ressources humaines est avisé du départ et collabore avec le personnel compétent pour que l'accès soit révoqué au moment du départ.
Départ à la retraite, si le dernier jour de travail est plusieurs semaines avant la date du départ	Le personnel des ressources humaines s'entend avec le gestionnaire sur la date où l'accès ne sera plus nécessaire et planifie la révocation de l'accès pour cette date.
Décès	Le personnel des ressources humaines est avisé du décès et collabore avec le personnel compétent pour entamer le processus de révocation.

Les mesures à prendre pour révoquer un accès comprennent notamment la suppression ou la désactivation des comptes utilisés par la ou les personnes. Les entités doivent considérer les ramifications d'une suppression de compte, lesquelles peuvent inclure des entrées de journaux d'événements incomplets en raison d'un compte non reconnu ou de services de système utilisant le compte pour se connecter.

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

Si une entité envisage de faire passer un employé contractuel à un statut d'employé permanent, elle doit se poser la question de l'obtention des pièces justificatives nécessaires pour respecter les exigences E1 à E4. S'il est impossible de fournir les pièces justificatives pour ces exigences, l'entité devrait se tourner vers les sous-critères pertinents de l'exigence E5 pour ce scénario de changement de statut administratif. Il serait souhaitable pour les entités d'inclure un tel scénario dans leur programme de gestion des accès, avec une approbation de niveau plus élevé afin de réduire au minimum les cas auxquels ce scénario s'appliquerait.

Exigence E6

Remarques générales sur l'exigence E6

Aucune

Directives d'application pour l'exigence E6

Cette exigence admet que le moment du départ peut varier selon les circonstances. Quelques scénarios courants et processus possibles selon le moment du départ sont présentés au tableau ci-dessous. Ces scénarios ne constituent pas une liste exhaustive de tous les scénarios possibles, mais ils sont représentatifs de plusieurs pratiques opérationnelles courantes.

Scénario	Processus possible
Départ involontaire immédiat	Un représentant des ressources humaines ou un agent de sécurité accompagne la personne hors du lieu de travail et le superviseur de celle-ci ou le personnel des ressources humaines demande au personnel compétent d'entamer le processus de révocation.
Départ involontaire prévu	Le personnel des ressources humaines est avisé du départ et collabore avec le personnel compétent pour que l'accès soit révoqué au moment du départ.
Départ volontaire	Le personnel des ressources humaines est avisé du départ et collabore avec le personnel compétent pour que l'accès soit révoqué au moment du départ.
Départ à la retraite, si le dernier jour de travail est plusieurs semaines avant la date du départ	Le personnel des ressources humaines s'entend avec le gestionnaire sur la date où l'accès ne sera plus nécessaire et planifie la révocation de l'accès pour cette date.
Décès	Le personnel des ressources humaines est avisé du décès et collabore avec le personnel compétent pour entamer le processus de révocation.

Les mesures à prendre pour révoquer un accès comprennent notamment la suppression ou la désactivation des comptes utilisés par la ou les personnes. Les entités doivent considérer les ramifications d'une suppression de compte, lesquelles peuvent inclure des entrées de journaux d'événements incomplets en raison d'un compte non reconnu ou de services de système utilisant le compte pour se connecter.

Pour assurer une séparation adéquate des tâches, l'autorisation et la fourniture d'accès ne doivent pas être assumées par la même personne dans la mesure du possible. La séparation des tâches doit également être prise en compte au moment de la vérification aux 15 mois civils selon l'exigence E6. La personne chargée de la vérification ne doit pas être celle qui fournit les accès.

Les entités peuvent choisir de ne pas fournir d'accès, ou de fournir des accès temporaires plutôt que permanents, aux utilisateurs autorisés. Autrement dit, il n'est pas nécessaire de fournir un accès à une personne autorisée ; par contre, tous les accès fournis doivent être autorisés.

Une entité peut choisir d'autoriser l'accès à certaines *BCSI*, ou encore d'appliquer des autorisations à certains emplacements de stockage ou types de *BCSI*.

L'autorisation prescrite à l'alinéa 6.1 porte uniquement sur la fourniture d'accès aux *BCSI* ; toutefois, les entités peuvent aussi vouloir établir un mécanisme pour autoriser les personnes (leur accorder une permission ou les rendre admissibles) à recevoir, à voir ou à utiliser des *BCSI* qui leur sont divulgués – à la manière d'une cote de sécurité. Un tel système peut contribuer à la protection de l'information, les personnes ayant pour consigne de ne partager des *BCSI* qu'avec d'autres personnes autorisées à en prendre connaissance ; les entités pourraient intégrer ce mécanisme à leur programme de protection de l'information dans le cadre de la norme CIP-011. Dans ce cas, la vérification prescrite à l'alinéa 6.2 de l'exigence E6 s'appliquerait quand même, et la révocation prescrite à l'alinéa 6.3 de l'exigence E6 pourrait consister à retirer le nom de la personne de la liste des autorisations au moment du départ ou à la suite d'un examen qui conclurait que le besoin d'accès n'existe plus pour la personne en question.

Les entités peuvent optimiser la vérification aux 15 mois des accès aux *BCSI* en mettant en place un accès basé sur les rôles. Cette méthode consiste à définir les rôles au sein du système (répartiteur, technicien, récepteur de rapports, administrateur, etc.), puis à grouper les droits d'accès selon ces différents rôles, et enfin à assigner leurs rôles aux utilisateurs. Ce système ne suppose aucun logiciel particulier et on peut le mettre en place en définissant des processus de fourniture d'accès particuliers pour chaque rôle ne permettant pas l'affectation de groupes de droits d'accès. Un exemple de calendrier de vérification aux 15 mois civils des autorisations d'accès aux *BCSI* est présenté sous forme graphique à la section *Directives d'application pour l'exigence E4*.

Exemple de départ géré selon l'alinéa 5.1 de l'exigence E5 et qui satisfait à l'alinéa 6.3 de l'exigence E6 : l'entité responsable retire la possibilité d'accès physique sans accompagnement et l'*accès distant interactif* de la personne (carte d'accès physique, réseau privé virtuel, compte Active Directory, etc.). Une fois retirés ses moyens d'accès physique et électronique, la personne perd la capacité d'accéder aux *informations de système électronique BES*. Il reste à l'entité responsable à révoquer tout accès fourni manuellement (compte d'utilisateur local, relais, serveur de réseau local, *BCSI* infonuagiques non liées à un compte Active Directory, etc.).

Annexe 1 : Guide d'application de la norme CIP-004-6

Cette section reproduit certaines portions du texte de la section *Principes directeurs et fondements techniques* de la norme CIP-004-6, à titre de référence historique. Par ailleurs, le texte de cette même section qui donne des indications sur l'intention de l'équipe de rédaction et sur la justification technique est reproduit dans un document intitulé *Justification technique de la norme de fiabilité CIP-004-7*.

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

Exigence E1

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

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

Exigence E2

L'entité responsable a la liberté de définir son propre programme de formation, qui peut comprendre plusieurs modules et modes de prestation, mais un seul programme de formation pour toutes les personnes à former est aussi acceptable. L'entité responsable peut, à sa guise, axer la formation sur les fonctions, les rôles ou les responsabilités.

Exigence E3

Le contrôle de l'identité doit être réalisé en respectant les lois fédérales, d'État, provinciales et locales ainsi que les ententes syndicales en vigueur.

Il peut s'agir, par exemple, de personnes de moins de 25 ans dont les antécédents à titre de jeune contrevenant sont protégés en vertu de la loi, de personnes qui ont résidé à des endroits où il est impossible d'obtenir des vérifications d'antécédents judiciaires ou de personnes dont l'emploi est régi par une convention collective qui l'interdit. Dans de tels cas, l'entité responsable doit tenir compte du fait que les renseignements sont incomplets lorsqu'elle évalue le risque d'accorder un accès.

Exigence E4

Pour assurer une séparation adéquate des tâches, l'autorisation et la fourniture d'accès ne doivent pas être assumées par la même personne dans la mesure du possible.

Pour ce faire, on compare la liste des personnes ayant reçu un accès à un *système électronique BES* avec le registre des personnes autorisées à accéder à ce *système électronique BES*. La liste des personnes ayant reçu un accès peut être une liste de comptes générée automatiquement. Toutefois, dans un *système électronique BES* comptant plusieurs bases de données de comptes, la liste des personnes ayant reçu un accès peut provenir d'autres sources, comme des activités de fourniture d'accès ou d'une base de données de comptes utilisateurs qui sert habituellement de point de départ à la fourniture des accès.

Les entités peuvent optimiser ce réexamen en mettant en place un accès basé sur les rôles. Cette méthode consiste à définir les rôles au sein du système (répartiteur, technicien, récepteur de

rapports, administrateur, etc.), puis à grouper les droits d'accès selon ces différents rôles, et enfin à assigner leurs rôles aux utilisateurs. Ce système ne suppose aucun logiciel particulier et on peut le mettre en place en définissant des processus de fourniture d'accès particuliers pour chaque rôle ne permettant pas l'affectation de groupes d'accès. Le système d'autorisation d'accès axé sur les rôles élimine la nécessité d'un réexamen des droits d'accès des comptes individuels.

Pour ce faire, on compare la liste des personnes auxquelles on a réellement fourni un accès à un *système électronique BES* avec le registre des personnes autorisées à accéder à ce *système électronique BES*. La liste des personnes auxquelles on a fourni un accès peut provenir d'une liste de comptes générée automatiquement. Toutefois, dans un *système électronique BES* comptant plusieurs bases de données de comptes, cette liste peut provenir d'autres sources, comme des activités de fourniture d'accès ou d'une base de données de comptes utilisateurs qui sert habituellement de point de départ à la fourniture des accès.

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

Exigence E5

Quelques scénarios courants et processus possibles selon le moment du départ sont présentés au tableau ci-dessous. Ces scénarios ne constituent pas une liste exhaustive de tous les scénarios possibles, mais ils sont représentatifs de plusieurs pratiques opérationnelles courantes.

Scénario	Processus possible
Départ involontaire immédiat	Un représentant des ressources humaines ou un agent de sécurité accompagne la personne hors du lieu de travail et le superviseur de celle-ci ou le personnel des ressources humaines demande au personnel compétent d'entamer le processus de révocation.
Départ involontaire prévu	Le personnel des ressources humaines est avisé du départ et collabore avec le personnel compétent pour que l'accès soit révoqué au moment du départ.
Départ volontaire	Le personnel des ressources humaines est avisé du départ et collabore avec le personnel compétent pour que l'accès soit révoqué au moment du départ.
Départ à la retraite, si le dernier jour de travail est plusieurs semaines avant la date du départ	Le personnel des ressources humaines s'entend avec le gestionnaire sur la date où l'accès ne sera plus nécessaire et planifie la révocation de l'accès pour cette date.
Décès	Le personnel des ressources humaines est avisé du décès et collabore avec le personnel compétent pour entamer le processus de révocation.

Les mesures à prendre pour ce faire comprennent notamment la suppression ou la désactivation des comptes utilisés par cette personne ; aucune mesure précise n'est cependant prescrite dans la norme. Les entités doivent considérer les ramifications d'une suppression de compte, lesquelles peuvent inclure des entrées de journaux d'événements incomplets en raison d'un compte non reconnu ou de services de système utilisant le compte pour se connecter.

Toutefois, rien n'empêche l'entité responsable de révoquer tous les accès au moment du départ.

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