Norme de fiabilité

(version française)

A. Introduction

1. **Titre :** Cybersécurité – Mécanismes de gestion de la sécurité

2. **Numéro :** CIP-003-9

3. **Objet :** Définir des mécanismes de gestion de la sécurité cohérents et viables qui établissent les responsabilités et l'imputabilité à l'égard de la protection des *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le *système de production-transport d'électricité* (*BES*).

4. **Applicabilité :**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.2.1.1. Système de DSF ou de DST qui :

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

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

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

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

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

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

4.2.3. **Exemptions :** Sont exemptés de la norme CIP-003-9 :

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 *périmètres de sécurité électronique* (*ESP*) 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, conformément 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.

5. Dates d'entrée en vigueur : Voir le plan de mise en œuvre de la norme CIP-003-9.

B. Exigences et mesures

E1. Chaque entité responsable doit réexaminer et faire approuver par un *cadre supérieur CIP*, au moins une fois tous les 15 mois civils, une ou plusieurs politiques de cybersécurité documentées qui, collectivement, couvrent les thèmes suivants :
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]

1.1. Pour ses *systèmes électroniques BES* à impact élevé ou moyen, le cas échéant :

1.1.1. personnel et formation (CIP-004) ;

1.1.2. *périmètres de sécurité électronique* (CIP-005), y compris l'*accès distant interactif ;*

1.1.3. sécurité physique des *systèmes électroniques BES* (CIP-006) ;

1.1.4. gestion de la sécurité des systèmes (CIP-007) ;

1.1.5. déclaration des incidents et planification des mesures d'intervention (CIP-008) ;

1.1.6. plans de rétablissement des *systèmes électroniques BES* (CIP-009) ;

1.1.7. gestion des changements de configuration et analyses de vulnérabilité (CIP-010) ;

1.1.8. protection de l'information (CIP-011) ; et

1.1.9. déclaration des *circonstances CIP exceptionnelles* et mesures d'intervention.

1.2. Pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, le cas échéant :

1.2.1. sensibilisation à la cybersécurité ;

1.2.2. contrôle de la sécurité physique ;

1.2.3. contrôle des accès électroniques ;

1.2.4. intervention en cas d'*incident de cybersécurité* ;

1.2.5. atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* et de *supports de stockage amovibles* ;

1.2.6. contrôles visant à sécuriser les accès électroniques distants des fournisseurs ; et

1.2.7. déclaration des *circonstances CIP exceptionnelles* et mesures d'intervention.

M1. Exemples non limitatifs de pièces justificatives : documents de politique ; historique de révisions, dossiers d'examen ou preuves de flux de travail provenant d'un système de gestion documentaire qui attestent le réexamen de chaque politique de cybersécurité au moins une fois tous les 15 mois civils ; et approbation documentée de chaque politique de cybersécurité par le *cadre supérieur CIP*.

E2. Chaque entité responsable qui détient au moins un actif comportant des *systèmes électroniques BES* à impact faible, selon les critères de la norme CIP-002, doit mettre en œuvre pour ses *systèmes électroniques BES* à impact faible un ou plusieurs plans de cybersécurité documentés comprenant toutes les sections de l'annexe 1.
[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]

Remarque : Un inventaire, une liste ou une désignation distincte des *systèmes électroniques BES* à impact faible ou de leurs *actifs électroniques BES* n'est pas exigé. Des listes d'utilisateurs autorisés ne sont pas exigées.

M2. Les pièces justificatives doivent comporter chacun des plans de cybersécurité qui, collectivement, couvrent toutes les sections de l'annexe 1 ; d'autres pièces justificatives doivent attester la mise en œuvre des plans de cybersécurité. L'annexe 2 présente d'autres exemples de pièces justificatives pour chacune des sections de l'annexe 1.

E3. Chaque entité responsable doit désigner nominativement un *cadre supérieur CIP* et documenter tout changement dans un délai de 30 jours civils suivant le changement.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]

M3. Exemple non limitatif de pièce justificative : document daté et approuvé par un haut dirigeant indiquant le nom de la personne désignée comme *cadre supérieur CIP*.

E4. L'entité responsable doit mettre en œuvre un processus documenté de délégation de pouvoirs, sauf en l'absence de toute délégation. Dans les cas permis par les normes CIP, le *cadre supérieur CIP* peut déléguer ses pouvoirs relatifs à certains actes à un ou plusieurs délégataires. Ces délégations doivent être documentées, et comprendre notamment le nom ou le titre du délégataire, les actes délégués et la date de la délégation ; être approuvées par le *cadre supérieur CIP* ; et être mises à jour dans un délai de 30 jours suivant tout changement à la délégation. Il n'est pas nécessaire de réaffirmer les changements de délégation en cas de changement de délégant.
[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]

M4. Exemple non limitatif de pièce justificative : document daté et approuvé par le *cadre supérieur CIP* indiquant la ou les personnes (nom ou titre) auxquelles est délégué le pouvoir d'approuver ou d'autoriser des actions décrites explicitement.

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 pour assurer la conformité* » (*CEA*) désigne la NERC ou l'*entité régionale* dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les *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 les 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. Programme de surveillance de la conformité et d'application des normes :

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

Niveaux de gravité de la non-conformité (VSL)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-9)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1.	**Planification de l'exploitation**	**Moyen**	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant l'un des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent. (E1.1) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant deux des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant le réexamen précédent. (E1.1) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant trois des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant le réexamen précédent. (E1.1) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant au moins quatre des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable n'avait aucune politique de cybersécurité documentée pour ses *systèmes électroniques BES* à impact élevé et moyen, comme le prescrit l'exigence E1. (E1.1) OU L'entité responsable n'a pas terminé le réexamen de sa ou ses politiques de cybersécurité selon l'exigence E1 dans un délai de 18 mois civils suivant le réexamen précédent. (E1) OU L'entité responsable n'a pas fait approuver par le *cadre*

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-9)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			selon l'exigence E1, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant l'approbation précédente. (E1.1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant un des sept thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils	selon l'exigence E1, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant l'approbation précédente. (E1.1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant deux des sept thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils	selon l'exigence E1, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant l'approbation précédente. (E1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant trois des sept thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils	*supérieur CIP* sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1 dans un délai de 18 mois civils suivant l'approbation précédente. (E1.1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant au moins quatre des sept thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable n'avait aucune politique de cybersécurité documentée, selon l'exigence E1, pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002. (E1.2)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-9)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant l'approbation précédente. (E1.2)	suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant l'approbation précédente. (E1.2)	suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant l'approbation précédente. (E1.2)	OU L'entité responsable n'a pas fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002 dans un délai de 18 mois civils suivant l'approbation précédente. (E1.2)
E2.	**Planification de l'exploitation**	**Faible**	L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté son plan de sensibilisation à la cybersécurité conformément à la section 1 de l'annexe 1 portant sur l'exigence E2. (E2) OU	L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas fait de rappel des pratiques de cybersécurité au moins une fois tous les 15 mois civils conformément à la section 1 de l'annexe 1 portant sur l'exigence E2. (E2)	L'entité responsable a documenté le contrôle des accès physiques pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas mis en place les mesures de sécurité physique conformément à la section 2 de l'annexe 1 portant sur l'exigence E2. (E2) OU	L'entité responsable n'a pas documenté et mis en œuvre un ou plusieurs plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible conformément à l'annexe 1 portant sur l'exigence E2. (E2)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-9)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			L'entité responsable a mis en place le contrôle des accès électroniques, mais n'a pas documenté son ou ses plans de cybersécurité concernant le contrôle des accès électroniques conformément à la section 3 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES*	OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté de mesures de sécurité physique conformément à la section 2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté de mesures de contrôle des accès électroniques conformément à la section 3 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité portant sur le contrôle des accès électroniques, mais n'a pas	L'entité responsable a documenté son ou ses plans de cybersécurité pour le contrôle des accès électroniques à ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas limité les communications aux seuls accès entrants et sortants nécessaires conformément à la section 3.1 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas mis à l'essai chaque plan d'intervention en cas d'*incident de cybersécurité* au moins une fois tous les 36 mois civils conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2)	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-9)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			à impact faible, mais n'a pas mis à jour chaque plan d'intervention en cas d'*incident de cybersécurité* dans un délai de 180 jours conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas géré ses *actifs électroniques temporaires* conformément à la section 5.1 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires*, mais n'a pas documenté les mesures applicables aux *supports de stockage amovibles* conformément à la section 5.3 de l'annexe 1	mis en place une authentification pour toute *connectivité par lien commuté* donnant accès à un ou des *systèmes électroniques BES* à impact faible, selon les capacités de l'*actif électronique*, conformément à la section 3.2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'incident dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas inclus le processus de détection, de classement et d'intervention en cas d'*incident de cybersécurité* conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans	OU L'entité responsable a documenté le processus consistant à déterminer si un *incident de cybersécurité* constaté est un *incident de cybersécurité à déclarer*, mais n'a pas avisé l'Electricity Information Sharing and Analysis Center (E-ISAC) conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* gérés par l'entité responsable conformément à la section 5.1 de l'annexe 1 portant sur l'exigence E2. (E2)	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-9)			
			VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
			portant sur l'exigence E2. (E2) OU L'entité responsable a mis en place des contrôles visant à sécuriser les accès électroniques distants des fournisseurs, mais n'a pas documenté son ou ses plans de cybersécurité concernant ces mesures conformément à la section 6 de l'annexe 1 portant sur l'exigence E2. (E2)	de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté le processus consistant à déterminer si un *incident de cybersécurité* constaté est un *incident de cybersécurité à déclarer*, puis à en aviser l'Electricity Information Sharing and Analysis Center (E-ISAC) conformément à la section 4 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* gérés par l'entité responsable conformément aux sections 5.1 et 5.3 de l'annexe 1 portant sur l'exigence E2. (E2)	OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable conformément à la section 5.2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures pour neutraliser la menace d'un programme malveillant détecté sur un *support de stockage amovible* avant de connecter celui-ci à un *système électronique BES* à	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-9)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				OU L'entité responsable a documenté son ou ses plans pour les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté de mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable conformément à la section 5.2 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en place de mesures applicables aux *supports de stockage amovibles* conformément à la section 5.3 de l'annexe 1 portant sur l'exigence E2. (E2)	impact faible conformément à la section 5.3 de l'annexe 1 portant sur l'exigence E2. (E2) OU L'entité responsable n'a pas documenté et mis en œuvre son ou ses plans de cybersécurité concernant les mesures de sécurité visant les accès électroniques distants des fournisseurs conformément à la section 6 de l'annexe 1 portant sur l'exigence E2. (E2)	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-9)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				OU L'entité responsable a documenté son ou ses plans de cybersécurité concernant les mesures de sécurité visant les accès électroniques distants des fournisseurs, mais n'a pas mis en place ces mesures conformément à la section 6 de l'annexe 1 portant sur l'exigence E2. (E2)		
E3.	**Planification de l'exploitation**	**Moyen**	L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais a documenté un changement concernant celui-ci dans un délai de plus de 30 jours civils et de moins de 40 jours civils suivant ce changement. (E3)	L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais a documenté un changement concernant celui-ci dans un délai de plus de 40 jours civils et de moins de 50 jours civils suivant ce changement. (E3)	L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais a documenté un changement concernant celui-ci dans un délai de plus de 50 jours civils et de moins de 60 jours civils suivant ce changement. (E3)	L'entité responsable n'a pas désigné nominativement un *cadre supérieur CIP*. OU L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais n'a pas documenté un changement concernant celui-ci dans un délai de 60 jours civils suivant ce changement. (E3)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-9)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E4.	**Planification de l'exploitation**	**Faible**	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 30 jours civils et de moins de 40 jours civils suivant ce changement. (E4)	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 40 jours civils et de moins de 50 jours civils suivant ce changement. (E4)	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 50 jours civils et de moins de 60 jours civils suivant ce changement. (E4)	L'entité responsable a délégué des pouvoirs relatifs à des actes autorisés par les normes CIP, mais n'a pas mis en œuvre de processus pour la délégation des actes du *cadre supérieur CIP*. (E4) OU L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais n'a pas documenté un changement à la délégation dans un délai de 60 jours civils suivant le changement. (E4)

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	Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'*entité régionale* comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « *responsable de la surveillance de la conformité* » par « *responsable des mesures pour assurer la conformité* ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Dans l'exigence E1.6, suppression de la phrase concernant le retrait du service d'un composant ou d'un système aux fins d'essais, en réponse à l'ordonnance de la FERC du 30 septembre 2009.	
3	16 décembre 2009	Approbation par le Conseil d'administration de la NERC.	
3	31 mars 2010	Approbation par la FERC.	
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	

Version	Date	Intervention	Suivi des modifications
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modification en coordination avec les autres normes CIP et révision du format selon le modèle RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-003-5.	
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.	Remplacement de la version adoptée par le Conseil le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux *systèmes électroniques BES* à impact faible.
6	21 janvier 2016	Ordonnance de la FERC approuvant la norme CIP-003-6 (dossier RM15-14-000).	
7	9 février 2017	Adoption par le Conseil d'administration de la NERC.	Révision en réponse à des prescriptions de l'ordonnance 822 de la FERC concernant 1) la définition de *LERC* et 2) les actifs temporaires.
7	19 avril 2018	Ordonnance de la FERC approuvant la norme CIP-003-7 (dossier RM17-11-000).	

Version	Date	Intervention	Suivi des modifications
8	9 mai 2019	Adoption par le Conseil d'administration de la NERC.	Suppression des références aux plans de défense. Changements en réponse aux prescriptions de l'ordonnance 843 de la FERC concernant l'atténuation des risques liés aux programmes malveillants.
8	31 juillet 2019	Ordonnance de la FERC approuvant la norme CIP-003-8 (dossier RD19-5-000).	
9	À déterminer	Révisions apportées pour donner suite à la résolution du Conseil d'administration de la NERC et au rapport sur la chaîne d'approvisionnement	

Annexe 1

Exigences des plans de cybersécurité pour les actifs comportant des *systèmes électroniques BES* à impact faible

Les entités responsables doivent intégrer chacune des sections suivantes aux plans de cybersécurité prescrits à l'exigence E2.

Les entités responsables dont les *systèmes électroniques BES* appartiennent à plusieurs catégories d'impact peuvent utiliser les politiques, procédures et processus adoptés pour leurs *systèmes électroniques BES* à impact élevé ou moyen pour leurs plans de cybersécurité visant les systèmes à faible impact. Chaque entité responsable peut élaborer des plans de cybersécurité pour des actifs individuels ou pour des groupes d'actifs.

Section 1. Sensibilisation à la cybersécurité : Chaque entité responsable doit rappeler, au moins une fois tous les 15 mois civils, les pratiques de cybersécurité (lesquelles peuvent comprendre des pratiques de sécurité physique connexes).

Section 2. Contrôle de la sécurité physique : Chaque entité responsable doit contrôler l'accès physique, d'après les besoins qu'elle détermine elle-même, 1) à l'actif ou aux emplacements des *systèmes électroniques BES* à impact faible à l'intérieur de l'actif, et 2) à tout *actif électronique* qu'elle décide d'affecter, conformément à la section 3.1, au contrôle des accès électroniques.

Section 3. Contrôle des accès électroniques : Pour chaque actif comportant un ou des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, l'entité responsable doit mettre en place un contrôle des accès électroniques qui :

3.1 autorise uniquement les accès entrants et sortants nécessaires, selon l'évaluation de l'entité responsable, pour toute communication :

i. entre un ou des *systèmes électroniques BES* à impact faible et tout *actif électronique* situé à l'extérieur de l'actif comportant un ou des *systèmes électroniques BES* à impact faible ;

ii. assurée par un protocole routable en entrée ou en sortie de l'actif comportant le ou les *systèmes électroniques BES* à impact faible ; et

iii. ne servant pas à des fonctions de commande ou de protection à délai critique entre des dispositifs électroniques intelligents (par exemple, des communications utilisant le protocole R-GOOSE de la norme CEI TR-61850-90-5) ;

3.2 authentifie toute *connectivité par lien commuté* donnant accès à des *systèmes électroniques BES* à impact faible, selon les capacités de l'*actif électronique*.

Section 4. Intervention en cas d'*incident de cybersécurité* : Chaque entité responsable doit avoir un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité*, par actif ou par groupe d'actifs, qui doivent comprendre :

4.1 la détection et le classement des *incidents de cybersécurité*, ainsi que les mesures d'intervention ;

4.2 le processus consistant à déterminer si un *incident de cybersécurité* détecté est un *incident de cybersécurité à déclarer*, puis à en aviser l'Electricity Information Sharing and Analysis Center (E-ISAC), à moins que la loi ne l'interdise ;

4.3 l'établissement des rôles et responsabilités des groupes ou des personnes chargés d'intervenir en cas d'*incident de cybersécurité* ;

4.4 la gestion des *incidents de cybersécurité* ;

4.5 la mise à l'essai des plans d'intervention en cas d'*incident de cybersécurité* au moins une fois tous les 36 mois civils : 1) en répondant à un *incident de cybersécurité à déclarer* réel ; 2) en effectuant un exercice d'entraînement ou sur table de réponse à un *incident de cybersécurité à déclarer* ; ou 3) en effectuant un exercice opérationnel de réponse à un *incident de cybersécurité à déclarer* ; et

4.6 la mise à jour des plans d'intervention en cas d'*incident de cybersécurité*, au besoin, dans les 180 jours civils suivant la mise à l'essai d'un plan d'intervention en cas d'*incident de cybersécurité* ou suivant un *incident de cybersécurité à déclarer* réel.

Section 5. Atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles* : Chaque entité responsable doit mettre en œuvre, sauf en cas de *circonstances CIP exceptionnelles*, un ou des plans visant à réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants dans les *systèmes électroniques BES* à impact faible à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*. Ce ou ces plans doivent comprendre :

5.1 pour tout *actif électronique temporaire* géré par l'entité responsable, le recours à un ou plusieurs des moyens suivants, utilisés en permanence ou à la demande (selon les capacités de l'*actif électronique temporaire*) :

- logiciel antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code ;
- liste blanche d'applications ; ou
- autres moyens d'atténuer le risque lié à l'introduction de programmes malveillants ;

5.2 pour tout *actif électronique temporaire* géré par une tierce partie autre que l'entité responsable :

5.2.1 l'application d'une ou de plusieurs des mesures suivantes avant de connecter l'*actif électronique temporaire* à un *système électronique BES* à impact faible (selon les capacités de l'*actif électronique temporaire*) :

- examen du degré de maintien à jour de l'antivirus ;
- examen de la procédure de mise à jour de l'antivirus adoptée par la tierce partie ;
- examen de l'utilisation par la tierce partie de listes blanches d'applications ;
- examen de l'utilisation de systèmes d'exploitation et de logiciels exécutables uniquement à partir de supports non inscriptibles ;
- examen des mesures de renforcement du système d'exploitation adoptées par la tierce partie ; ou

- autres moyens d'atténuation du risque lié à l'introduction de programmes malveillants ;

5.2.2 pour toute méthode utilisée conformément à la section 5.2.1, les entités responsables doivent déterminer si des mesures d'atténuation supplémentaires sont nécessaires, et les mettre en œuvre avant de connecter l'*actif électronique temporaire* ;

5.3 pour les *supports de stockage amovibles*, le recours à chacun des moyens suivants :

5.3.1 mesures permettant de détecter les programmes malveillants sur les *supports de stockage amovibles* au moyen d'un *actif électronique* autre qu'un *système électronique BES* ; et

5.3.2 mesures permettant de neutraliser la menace d'un programme malveillant détecté sur un *support de stockage amovible* avant de connecter ce support à un *système électronique BES* à impact faible.

Section 6. Contrôles visant à sécuriser les accès électroniques distants des fournisseurs : Pour les actifs comportant un ou des *systèmes électroniques BES* à impact faible désignés comme tels selon les critères de la norme CIP-002 et qui permettent l'accès électronique distant à des fournisseurs, l'entité responsable doit mettre en œuvre un processus pour atténuer les risques associés à cet accès, lequel est défini à la section 3.1. Ce processus doit prévoir :

6.1 une ou plusieurs méthodes permettant d'identifier les accès électroniques distants des fournisseurs ;

6.2 une ou plusieurs méthodes permettant de désactiver les accès électroniques distants des fournisseurs ;

6.3 une ou plusieurs méthodes permettant de détecter les communications malveillantes, entrantes et sortantes, reconnues ou présumées pour les accès électroniques distants des fournisseurs.

Annexe 2

Plans de cybersécurité pour les actifs comportant des *systèmes électroniques BES* à impact faible – Exemples de pièces justificatives

Section 1. Sensibilisation à la cybersécurité : Exemples non limitatifs de pièces justificatives pour la section 1 : documentation attestant que le rappel des pratiques de cybersécurité a été fait au moins une fois tous les 15 mois civils. Les pièces justificatives peuvent porter sur une ou plusieurs des méthodes suivantes :

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

Section 2. Contrôle de la sécurité physique : Exemples non limitatifs de pièces justificatives pour la section 2 :

- documentation des mécanismes de contrôle d'accès (carte d'accès, serrures, sécurisation de périmètre, etc.), des mesures de surveillance (systèmes d'alarme, surveillance humaine, etc.) ou d'autres mesures de sécurité physique de nature opérationnelle, administrative ou technique pour le contrôle de l'accès physique :
    a. à l'actif, s'il y a lieu, ou aux emplacements de *système électronique BES* à impact faible à l'intérieur de l'actif ; et
    b. à tout *actif électronique* désigné par l'entité responsable comme assurant un contrôle des accès électroniques selon la section 3.1 de l'annexe 1, s'il y a lieu.

Section 3. Contrôle des accès électroniques : Exemples non limitatifs de pièces justificatives pour la section 3 :

1. documentation attestant qu'à chaque actif ou groupe d'actifs comportant des *systèmes électroniques BES* à impact faible, toute communication routable entre un ou plusieurs de ces *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* à l'extérieur de l'actif en question est limitée par un contrôle des accès électroniques aux seuls accès électroniques entrants et sortants que l'entité responsable juge nécessaires, sauf si l'entité peut démontrer qu'il s'agit d'une communication utilisée pour des fonctions de commande ou de protection à délai critique entre des dispositifs électroniques intelligents. Exemples non limitatifs de pièces justificatives : schémas montrant le contrôle des communications entrantes et sortantes entre le ou les *systèmes électroniques BES* à impact faible et un ou des *actifs électroniques* situés à l'extérieur de l'actif comportant ce ou ces *systèmes électroniques BES*, ou des listes de contrôle des accès électroniques mises en œuvre (contrôles d'accès par adresse IP, par ports ou par service, passerelles unidirectionnelles, etc.) ;
2. documentation du mécanisme d'authentification de la *connectivité par lien commuté* (appels sortants limités à un numéro préprogrammé pour la transmission de données, modems à fonction de rappel, modems télécommandés par le *centre de contrôle* ou la salle de commande, contrôle d'accès dans le *système électronique BES*, etc.).

Section 4. Intervention en cas d'*incident de cybersécurité :* Exemples non limitatifs de pièces justificatives pour la section 4 : documents datés (politiques, procédures, processus, etc.)

d'un ou de plusieurs plans d'intervention en cas d'*incident de cybersécurité* établis par actif ou par groupe d'actifs, qui comprennent les actions suivantes :

1. détecter les *incidents de cybersécurité*, les classer et y répondre ; déterminer si un *incident de cybersécurité* détecté est un *incident de cybersécurité à déclarer* et aviser l'Electricity Information Sharing and Analysis Center (E-ISAC) ;
2. établir et documenter les rôles et responsabilités des groupes ou des personnes chargés d'intervenir en cas d'*incident de cybersécurité* (déclenchement, documentation, surveillance, déclaration, etc.) ;
3. gérer les *incidents de cybersécurité* (confinement, élimination, reprise après incident ou résolution de l'incident, etc.) ;
4. mettre à l'essai le ou les plans, avec documents datés attestant qu'un essai a été fait au moins une fois tous les 36 mois civils ; et
5. mettre à jour au besoin les plans d'intervention en cas d'*incident de cybersécurité* dans les 180 jours civils suivant la mise à l'essai ou suivant un *incident de cybersécurité à déclarer* réel.

Section 5. Atténuation des risques liés à l'introduction de programmes malveillants à partir d'*actifs électroniques temporaires* ou de *supports de stockage amovibles* :

1. Exemples non limitatifs de pièces justificatives attestant la conformité avec la section 5.1 : documentation des moyens utilisés pour atténuer le risque lié à l'introduction de programmes malveillants, comme des logiciels antivirus et des processus de gestion des mises à jour des signatures ou des séquences de code, des pratiques de liste blanche d'applications, des processus de restriction des communications ou d'autres moyens d'atténuation appropriés. Si un *actif électronique temporaire* n'a pas la capacité de mettre en place certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation du fournisseur ou de l'entité responsable indiquant que l'*actif électronique temporaire* n'a pas cette capacité.
2. Exemples non limitatifs de pièces justificatives attestant la conformité avec la section 5.2.1 : documentation provenant de systèmes de gestion des changements, courriels ou procédures qui documentent un examen du degré de maintien à jour des antivirus installés ; notes de service, courriels, documentation de système, politiques ou contrats d'une tierce partie autre que l'entité responsable qui décrivent le processus de mise à jour des antivirus, l'utilisation d'une liste blanche d'applications, l'utilisation de systèmes d'exploitation sur support externe ou le renforcement du système d'exploitation par la tierce partie ; pièces justificatives provenant de systèmes de gestion des changements, courriels ou contrats indiquant que l'entité responsable juge acceptables les pratiques de la tierce partie ; ou documentation d'autres moyens d'atténuation du risque lié à l'introduction de programmes malveillants pour les *actifs électroniques temporaires* gérés par la tierce partie. Si un *actif électronique temporaire* n'a pas la capacité de mettre en place certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation de l'entité responsable ou de la tierce partie indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Exemples non limitatifs de pièces justificatives attestant la conformité avec la section 5.2.2 de l'annexe 1 : documentation provenant de systèmes de gestion des changements, courriels ou contrats attestant qu'un examen a été effectué pour déterminer le besoin de mesures d'atténuation supplémentaires, et que ces mesures, le cas échéant, ont été mises en œuvre avant la connexion de l'*actif électronique temporaire* géré par une tierce partie autre que l'entité responsable.

3. Exemples non limitatifs de pièces justificatives attestant la conformité avec la section 5.3.1 : processus documentés des moyens de détection des programmes malveillants, comme les résultats de balayage paramétré pour les *supports de stockage amovibles* ou la mise en œuvre du balayage à la demande. Exemples non limitatifs de pièces justificatives attestant la conformité avec la section 5.3.2 : processus documentés des moyens d'atténuation du risque lié aux programmes malveillants détectés sur les *supports de stockage amovibles*, comme les journaux créés par les mécanismes de détection qui montrent les résultats du balayage et indiquent la neutralisation des programmes malveillants détectés sur les *supports de stockage amovibles*, ou une confirmation documentée par l'entité que les *supports de stockage amovibles* sont considérés comme exempts de tout programme malveillant.

Section 6. Mesures de sécurité visant les accès électroniques distants des fournisseurs. Exemples non limitatifs de pièces justificatives attestant la mise en œuvre du processus indiqué à la section 6 :

1. Pour la section 6.1, la documentation attestant :
   - les étapes de préautorisation des accès ;
   - les alertes générées lors de l'ouverture d'une session par les fournisseurs ;
   - la surveillance des sessions ;
   - la journalisation des alertes de changement à la gestion des informations de sécurité ;
   - l'ouverture de session en cas de besoins ponctuels ;
   - l'enregistrement des sessions ;
   - les registres du système ; ou
   - les autres mesures de nature opérationnelle, administrative ou technique employées.
2. Pour la section 6.2, la documentation attestant :
   - la désactivation de comptes utilisateurs ou de comptes système qui permettent l'accès électronique distant des fournisseurs ;
   - la désactivation de ports d'entrée ou de sortie matériels ou logiciels, de services, ou de permissions d'accès dans des applications, des pare-feu, des systèmes de détection et de prévention des intrusions (IDS/IPS), des routeurs, des commutateurs, des réseaux privés virtuels (VPN), l'application Remote Desktop, des télécommandes, ou tout autre matériel ou logiciel utilisé pour permettre l'accès électronique distant de fournisseurs ;
   - la désactivation de protocoles de communications (notamment IP) utilisés par des systèmes qui établissent ou maintiennent l'accès électronique distant de fournisseurs ;
   - la suppression de la connectivité de la couche physique (p. ex., déconnexion d'un câble Ethernet, mise hors tension d'un équipement) ;
   - les mesures administratives définissant les méthodes, les étapes ou les systèmes utilisés pour désactiver l'accès électronique distant de fournisseurs ; ou
   - les autres mesures de nature opérationnelle, administrative ou technique employées.

3. Pour la section 6.3, la documentation attestant la mise en place de processus ou de technologies capables de détecter les communications malveillantes, tels que les suivants :
   - anti-logiciels malveillants ;
   - système de détection des intrusions (IDS) et système de prévention des intrusions (IPS) ;
   - examen automatisé ou manuel des journaux ;
   - systèmes d'alerte ; ou
   - autres mesures de nature opérationnelle, administrative ou technique.