**Formulaire d’audit de la norme de fiabilité au Québec**

# CIP-003-8 — Mécanismes de gestion de la sécurité

***Cette section doit être complétée par le NPCC.***

|  |  |
| --- | --- |
| **Numéro de l’audit:** | NPCC-NIRnnnn-YYYYMMDD |
| **Entité visée:** | Nom de l’entité visée |
| **Numéro d’identification à la Régie:** | NIRnnnn |
| **Responsable des mesures pour assurer la conformité:** | Régie de l’énergie |
| **Date(s)**[[1]](#footnote-1) **d’évaluation de la conformité:** | Du jour mois année au jour mois année |
| **Processus de surveillance de la conformité:** | [Audit sur place | Audit hors site | Contrôle ponctuel] |
| **Noms des auditeurs:** | Fournis par le NPCC |

Applicabilité des exigences:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **BA** | **DP** | **GO** | **GOP** | **LSE** | **PA** | **RC** | **RP** | **TO** | **TOP** | **TP** | **TSP** |
| **E1** | **X** | **\*** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |
| **E2** | **X** | **\*** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |
| **E3** | **X** | **\*** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |
| **E4** | **X** | **\*** | **X** | **X** |  |  | **X** |  | **X** | **X** |  |  |

**\*** CIP-003-8 s’applique uniquement aux *DP* qui possèdent certains DSF*,* DST, *RAS*, *systèmes de protection* ou *chemins de démarrage*. Voir CIP-003-8 Section 4, Applicabilité, pour plus de détails.

**Légende:**

|  |  |
| --- | --- |
| Texte avec fond bleu: | Texte figé – ne pas modifier |
| Zone d’entrée de texte avec fond vert: | Information fournie par l’entité |
| Zone d’entrée de texte avec fond blanc: | Information fournie par l’auditeur |

**Clause de non-responsabilité**

Ce formulaire d’audit de la norme de fiabilité au Québec (formulaire) a été conçu pour faciliter l’évaluation, par le NPCC, de la conformité à cette norme de fiabilité et son annexe (l’Annexe) d’une entité visée au Québec. Ce formulaire contient toutes les questions et tous les sujets pertinents du formulaire correspondant de la NERC utilisé aux États-Unis. Le texte du formulaire est adapté aux versions spécifiques de chaque norme de fiabilité. Les entités qui utilisent ce formulaire devraient choisir la version du formulaire qui s’applique à la norme de fiabilité qui est évaluée. Bien que l’information contenue dans ce formulaire dévoile en partie la méthodologie que le NPCC a choisie pour évaluer la conformité aux exigences de la norme de fiabilité, ce document ne doit pas remplacer la norme de fiabilité ou ne doit pas être vu comme un ajout d’exigences à la norme de fiabilité. Dans tous les cas, l’entité régionale doit se baser sur le texte de la norme de fiabilité elle-même et non sur le texte de ce formulaire, pour déterminer la conformité à la norme de fiabilité. Les normes de fiabilité peuvent être consultées [sur le site internet de la Régie](http://www.regie-energie.qc.ca/audiences/NormesFiabiliteTransportElectricite/NormesFiabilite.html). Par ailleurs, les normes de fiabilité sont fréquemment mises à jour et il se peut que ce formulaire ne soit pas mis à jour à la même fréquence. Par conséquent, il est impératif que les entités visées considèrent ce formulaire comme un document de référence seulement et non comme un suppléant ou remplaçant de la norme de fiabilité. Il est de la responsabilité de l’entité visée de vérifier si elle est conforme à la dernière version approuvée, par l’autorité gouvernementale applicable, de la norme de fiabilité, en fonction de son inscription [au registre des entités](http://www.regie-energie.qc.ca/audiences/NormesFiabiliteTransportElectricite/RegistreEntites.html).

Ce formulaire fournit, à titre d’information seulement, une liste non-exclusive d’exemples de types de pièces justificatives qu’une entité visée pourrait devoir fournir ou pourrait être demandée de fournir pour démontrer la conformité à la norme de fiabilité. Les pièces justificatives soumises par l’entité visée pour répondre aux exemples de ce formulaire n’assurent pas nécessairement la conformité à la norme de fiabilité, et le NPCC se réserve le droit de demander des pièces justificatives additionnelles, non contenue dans le formulaire, de la part de l’entité visée.

Constats

**(Cette section doit être complétée par le NPCC)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Exig.** | **Constat** | **Résumé et documentation** | **Fonctions surveillées** |
| **E1** |  |  |  |
| **E2** |  |  |  |
| **E3** |  |  |  |
| **E4** |  |  |  |

|  |  |
| --- | --- |
| **Exig.** | **Sujets de préoccupation** |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| **Exig.** | **Recommandations** |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| **Exig.** | **Observations positives** |
|  |  |
|  |  |
|  |  |

**Experts en la matière**

Identifier le ou les experts en la matière, responsables de la norme de fiabilité.

**Réponse de l’entité visée (Requise; Veuillez insérez des lignes supplémentaires, si nécessaire) :**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nom de l’expert en la matière** | **Titre** | **Organisation** | **Exigence(s)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**E1 Documentation et pièces justificatives à l’appui**

**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. Pour ses *systèmes électroniques BES* à impact élevé ou moyen, le cas échéant :
     1. personnel et formation (CIP-004) ;
     2. *périmètres de sécurité électronique* (CIP-005), y compris l’*accès distant interactif ;*
     3. sécurité physique des *systèmes électroniques BES* (CIP-006) ;
     4. gestion de la sécurité des systèmes (CIP-007) ;
     5. déclaration des incidents et planification des mesures d’intervention (CIP-008) ;
     6. plans de rétablissement des *systèmes électroniques BES* (CIP-009) ;
     7. gestion des changements de configuration et analyses de vulnérabilité (CIP‑010) ;
     8. protection de l’information (CIP-011) ; et
     9. déclaration des *circonstances* CIP *exceptionnelles* et mesures d’intervention.
  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. sensibilisation à la cybersécurité ;
     2. mesures de sécurité physique ;
     3. contrôle des accès électroniques ;
     4. intervention en cas d’*incident de cybersécurité*;
     5. atténuation des risques liés à l’introduction de programmes malveillants à partir d’*actifs électroniques temporaires* et de *supports de stockage amovibles*; et
     6. 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.

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

|  |
| --- |
|  |
|  |
|  |

**Démarche d’évaluation de la conformité spécifique à la norme CIP-003-8, E1**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Pour ses *systèmes électroniques BES* à impact élevé ou moyen, le cas échéant, vérifier que l’entité responsable a documenté une ou plusieurs politiques de cybersécurité qui, collectivement, couvrent les thèmes suivants :   * + 1. personnel et formation (CIP-004) ;     2. *périmètres de sécurité électronique* (CIP-005), y compris l’*accès distant interactif ;*     3. sécurité physique des *systèmes électroniques BES* (CIP-006) ;     4. gestion de la sécurité des systèmes (CIP-007) ;     5. déclaration des incidents et planification des mesures d’intervention (CIP-008) ;     6. plans de rétablissement des *systèmes électroniques BES* (CIP-009) ;     7. gestion des changements de configuration et analyses de vulnérabilité (CIP-010) ;     8. protection de l’information (CIP-011) ; et     9. déclaration des *circonstances CIP exceptionnelles* et mesures d’intervention. |
|  | Pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, le cas échéant, vérifier que l’entité responsable a documenté une ou plusieurs politiques de cybersécurité qui, collectivement, couvrent les thèmes suivants :   * + 1. sensibilisation à la cybersécurité ;     2. mesures de sécurité physique ;     3. contrôle des accès électroniques ;     4. intervention en cas d’*incident de cybersécurité*;     5. atténuation des risques liés à l’introduction de programmes malveillants à partir d’*actifs électroniques temporaires* et de *supports de stockage amovibles* ; et     6. déclaration des *circonstances CIP exceptionnelles* et mesures d’intervention. |
|  | Vérifier que chaque politique utilisée pour répondre à cette exigence a été réexaminée au moins une fois tous les 15 mois civils. |
|  | Vérifier que le *cadre supérieur CIP* a approuvé chaque politique utilisée pour répondre à cette exigence, au moins une fois tous les 15 mois civils. |
|  | Vérifier que l’entité responsable a atteint l’objectif de sécurité qui consiste à établir des politiques de cybersécurité qui préservent la disponibilité, l’intégrité et la confidentialité des systèmes afin de permettre l’exploitation fiable du *BES*. |
| **Notes pour l’auditeur :**  Selon l’annexe 1 : « 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. » | |

**Notes des auditeurs:**

**E2 Documentation et pièces justificatives à l’appui**

**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* BESà 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.

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

|  |
| --- |
|  |
|  |
|  |

**Démarche d’évaluation de la conformité spécifique à la norme CIP-003-8, E2**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Annexe 1, section 1  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a documenté un plan afin de rappeler les pratiques de cybersécurité (lesquelles peuvent comprendre des pratiques de sécurité physiques connexes) au moins une fois tous les 15 mois civils. |
|  | Annexe 1, section 1  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a mis en œuvre son plan afin de rappeler les pratiques de cybersécurité (lesquelles peuvent comprendre des pratiques de sécurité physiques connexes) au moins une fois tous les 15 mois civils. |
|  | Annexe 1, section 1  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a atteint l’objectif de sécurité qui consiste à s’assurer que le personnel ayant accès aux *systèmes électroniques BES* à impact faible demeure au fait des pratiques de cybersécurité. |
|  | Annexe 1, section 2  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a documenté un plan pour contrôler l’accès physique d’après les besoins qu’elle a déterminés 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,* désigné par l’entité responsable, qui assure le ou les contrôles des accès électroniques conformément à la section 3.1 de l’annexe 1, s’il y a lieu. |
|  | Annexe 1, section 2  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a mis en œuvre son plan pour contrôler l’accès physique. |
|  | Annexe 1, section 2  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a atteint l’objectif de sécurité qui consiste à contrôler l’accès physique:   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*, désigné par l’entité responsable, qui assure le ou les contrôles des accès électroniques conformément à la section 3.1 de l’annexe 1, s’il y a lieu. |
|  | Annexe 1, section 3.1  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a documenté un plan pour contrôler les accès entrants et sortants, d’après les besoins qu’elle a déterminés elle-même, pour toute communication :   1. 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 ; 2. assurée par un protocole routable en entrée ou en sortie de l’actif comportant le ou les *systèmes électroniques* *BES* à impact faible ; et 3. 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 CEITR-61850-90-5). |

|  |  |
| --- | --- |
|  | Annexe 1, section 3.1  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a mis en œuvre son plan pour contrôler les accès électroniques. |
|  | Annexe 1, section 3.1  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a atteint l’objectif de sécurité qui consiste à autoriser uniquement les accès entrants et sortants nécessaires à ses *systèmes électroniques* *BES* à impact faible. |
|  | Annexe 1, section 3.2  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a documenté un plan pour authentifier toute *connectivité par lien commuté*, le cas échéant, donnant accès à des *systèmes électroniques* *BES* à impact faible, selon les capacités de l’*actif électronique*. |
|  | Annexe 1, section 3.2  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a mis en œuvre le plan pour authentifier toute *connectivité par lien commuté*. |
|  | Annexe 1, section 3.2  Pour chaque actif comportant un *système électronique BES* à impact faible, vérifier que l’entité responsable a atteint l’objectif de sécurité qui consiste à authentifier toute *connectivité par lien commuté*, selon les capacités de l’*actif électronique*, lorsqu’une telle connectivité permet l’accès à ses *systèmes électroniques BES* à impact faible. |
|  | Annexe 1, section 4  Pour chaque actif comportant des *systèmes électroniques BES* à impact faible, vérifier que l’entité responsable a documenté un ou plusieurs plans d’intervention en cas d’*incident de cybersécurité* qui comprennent :   1. la détection et le classement des *incidents de cybersécurité*, ainsi que les mesures d’intervention ; 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 ; 3. l’établissement des rôles et responsabilités des groupes ou des personnes chargés d’intervenir en cas d’*incident de cybersécurité* ; 4. la gestion des *incidents de cybersécurité* ; 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 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. |
|  | Annexe 1, section 4  Pour chaque actif comportant des *systèmes électroniques BES* à impact faible, lorsque l’entité responsable a agi en cas d’*incident de cybersécurité*, vérifier que l’entité responsable a mis en œuvre son plan d’intervention en cas d’*incident de cybersécurité*. |

|  |  |
| --- | --- |
|  | Annexe 1, section 4.5  Vérifier que l’entité responsable a mis à l’essai chaque plan 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*. |
|  | Annexe 1, section 4.6  Vérifier que l’entité responsable a mis à jour chaque plan d’intervention en cas d’*incident de cybersécurité*, au besoin, dans un délai de 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. |
|  | Annexe 1, section 4  Vérifier que l’entité responsable est prête à atteindre l’objectif de sécurité qui consiste à minimiser l’impact négatif en cas d’un possible *incident de cybersécurité* sur le *BES* affectant des *systèmes électroniques BES* à impact faible. |
|  | Annexe 1, sections 5.1, 5.2 et 5.2.1  Vérifier que l’entité responsable a documenté un ou plusieurs plans visant à atténuer le risque lié à l’introduction de programmes malveillants dans les *systèmes électroniques* *BES* à impact faible à partir d’*actifs électroniques temporaires.* |
|  | Annexe 1, sections 5.1, 5.2 et 5.2.1  Vérifier que l’entité responsable a mis en œuvre ses plans visant à atténuer le risque lié à l’introduction de programmes malveillants dans les *systèmes électroniques* *BES* à impact faible à partir d’*actifs électroniques temporaires.* |
|  | Annexe 1, sections 5.1, 5.2 et 5.2.1  Vérifier que l’entité responsable a atteint l’objectif qui consiste à atténuer le risque lié à l’introduction de programmes malveillants dans les *systèmes électroniques* *BES* à impact faible à partir d’*actifs électroniques temporaires.* |
|  | Annexe1, section 5.2.2  Pour toute méthode utilisée conformément à la section 5.2.1, vérifier que l’entité responsable a déterminé si des mesures d’atténuation supplémentaires sont nécessaires et les a mis en œuvre avant de connecter l’*actif électronique temporaire.* |
|  | Annexe 1, section 5.3.1  Vérifier que l’entité responsable a documenté un ou des plans permettant de détecter tout programme malveillant sur les *supports de stockage amovibles* au moyen d’un *actif électronique* autre qu’un *système électronique BES*. |
|  | Annexe 1, section 5.3.2  Vérifier que l’entité responsable a documenté un ou des plans 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. |
|  | Annexe 1, section 5.3  Vérifier que l’entité responsable a mis en œuvre ses plans visant à atténuer les risques lié à l’introduction de programmes malveillants dans les *systèmes électroniques* *BES* à impact faible à partir de *supports de stockage amovibles.* |

|  |  |
| --- | --- |
|  | Annexe 1, section 5.3  Vérifier que l’entité responsable a atteint l’objectif qui consiste à atténuer le risque lié à l’introduction de programmes malveillants dans les *systèmes électroniques* *BES* à impact faible à partir de *supports de stockage amovibles.* |
| **Notes pour l’auditeur :**  Annexe 1, section 3   1. Pour chaque actif comportant un ou des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, la liste des actifs devrait identifier les actifs qui ont des communications par protocole routable 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 en entrée ou en sortie de l’actif, et qui ne servent pas pour assurer des fonctions de protection ou de commande à délai critique. 2. Pour ces actifs identifiés, obtenir comme pièce justificative les dispositifs utilisés pour le contrôle des accès électroniques et les *systèmes électroniques BES* à impact faible pour lesquels ils contrôlent l’accès. 3. Pour chaque actif comportant un ou des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, l’entité responsable a l’obligation de déterminer les communications par protocole routable entrantes et sortantes nécessaires entre un ou des *systèmes électronique 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 en entrée ou en sortie de l’actif et qui ne servent pas à des fonctions de commande ou de protection à délai critique. L’entité responsable doit être en mesure de fournir une explication techniquement valable sur comment les autorisations et le contrôle des accès électroniques concordent avec l’objectif de sécurité qui consiste à autoriser uniquement les accès entrants et sortants nécessaires aux *systèmes électroniques BES* à impact faible. 4. L’équipe d’audit devrait évaluer l’efficacité du plan de contrôle des accès électroniques de l’entité responsable de même que son exécution conforme. 5. Pour les communications entrantes et sortantes que l’entité responsable a jugé nécessaires, l’entité responsable doit identifier les contrôles des accès électroniques utilisés pour contrôler efficacement l’accès vers un ou des *systèmes électroniques BES* à impact faible ou à partir de ceux-ci. 6. Les dix modèles de référence inclus à la section Principes directeurs et fondements techniques de la norme présentent des exemples auxquels les entités responsables peuvent se référer pour leur contrôle des accès électroniques. Les modèles de référence 9 et 10 présentent les approches de segmentation du trafic réseau de manière à n’avoir aucune communication par protocole routable vers le ou les *systèmes électroniques BES* à impact faible.    1. Le modèle 9 utilise la segmentation de réseau à deux couches (VLANs) pour contrôler l’accès. La configuration des dispositifs utilisée pour accomplir ceci doit être documentée par l’entité responsable et évaluée pour son efficacité à atteindre les objectifs de la norme en terme de contrôle des accès à un ou des *systèmes électroniques* *BES* à impact faible.    2. Dans le modèle 10, un seul dispositif reçoit à la fois le trafic série destiné à un ou des *systèmes électroniques BES* à impact faible et le trafic routable destiné à un ou des actifs électroniques non-BES. Le dispositif, tel que décrit dans le modèle, isole logiquement le trafic série du trafic routable. Les configurations du dispositif doivent être documentées par l’entité responsable et évaluées pour déterminer si les contrôles des accès électroniques répondent, ou non, efficacement aux objectifs de contrôle des accès aux *systèmes électroniques BES* à impact faible.   Annexe 1, section 5   1. Les moyens de vérifier l’atténuation des risques liés à l’introduction de programmes malveillants dans les *systèmes électroniques BES* à impact faible diffèrent selon le mode de gestion, en continu ou sur demande, de l’*actif électronique* *temporaire* par l’entité responsable. La vérification d’un *actif électronique* *temporaire* géré en continu est axée sur le moyen de prévenir l’introduction de programmes malveillants dans l’*actif électronique temporaire*. La vérification d’un *actif électronique temporaire* géré sur demande est axée sur le processus utilisé pour s’assurer que l’*actif électronique temporaire* peut être utilisé de manière sécuritaire dans l’environnement d’un *système électronique BES* à impact faible avant cet usage. Si l’*actif électronique temporaire* est géré à la fois sur demande et en continu, alors les deux techniques de vérification devraient être utilisées. | |

**Notes des auditeurs:**

**E3 Documentation et pièces justificatives à l’appui**

**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*.

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

|  |
| --- |
|  |
|  |
|  |

**Démarche d’évaluation de la conformité spécifique à la norme CIP-003-8, E3**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que le *cadre supérieur CIP* a été désigné nominativement. |
|  | Vérifier que tout changement à la désignation du *cadre supérieur CIP* a été daté et documenté dans un délai de 30 jours suivant le changement. |
|  | Vérifier que le *cadre supérieur CIP* désigné est l’unique cadre supérieur de la direction ayant l’autorité et la responsabilité pour mener et gérer la mise en œuvre et le respect continu des exigences des normes CIP de la NERC, CIP-002 à CIP-011. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E4 Documentation et pièces justificatives à l’appui**

**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.

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

|  |
| --- |
|  |
|  |
|  |

**Démarche d’évaluation de la conformité spécifique à la norme CIP-003-8, E4**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un processus de délégation de pouvoirs, sauf en l’absence de toute délégation. |
|  | Vérifier que l’ensemble des délégataires ont été désignés nominativement ou par leur titre. |
|  | Vérifier que la délégation des pouvoirs comprend l’acte spécifique délégué. |
|  | Vérifier que les actes spécifiques délégués par le *cadre supérieur CIP* sont permis par les normes CIP. |
|  | Vérifier que les dates de toutes les délégations ont été consignées. |
|  | Vérifier que le *cadre supérieur CIP* a approuvé toutes les délégations. |
|  | Vérifier que tous les changements aux délégations ont été datés et documentés dans un délai de 30 jours civils suivant ces changements. |
| **Notes pour l’auditeur :** La délégation de pouvoirs du *cadre supérieur CIP* est permise pour les approbations requises dans le cadre des normes CIP-002-5.1a, exigence E2, CIP-007-6, exigence E2, alinéa 2.4, et CIP-013-1 exigence E3. | |

**Notes des auditeurs:**

**Information supplémentaire**

**Norme de fiabilité**

Le texte complet de la norme CIP-003-8 peut être consulté sur le site internet de la Régie de l’énergie, à la section [surveillance de la conformité](http://www.regie-energie.qc.ca/audiences/NormesFiabiliteTransportElectricite/index.html).



**Historique des révisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Réviseurs** | **Description de la révision** |
| 1 | Septembre 2021 | Document initial | Document créé à partir du formulaire « RSAW » de la NERC |
| 2 | Février 2022 | Régie de l’énergie | Changement de gabarit |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Date(s) d’évaluation de la conformité: la ou les dates auxquelles l’évaluation de la conformité réelle (audit sur place, audit hors site, contrôle ponctuel, etc.) a lieu. [↑](#footnote-ref-1)