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

# CIP-008-6 — Cybersécurité – Déclaration des incidents et planification des mesures d’intervention

***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** |  |  |

\* La norme CIP-008-6 s’applique uniquement aux *distributeurs* qui ont certains systèmes de délestage de *charge* en sous-fréquence (DSF), systèmes de délestage de *charge* en sous-tension (DST), *automatismes de réseau* (RAS), systèmes de protection ou *chemins de* *démarrage*. Voir la Section 4, Applicabilité, de la norme CIP-008-6 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** |  |  |  |
| A1.1 |  |  |  |
| A1.2 |  |  |  |
| A1.3 |  |  |  |
| A1.4 |  |  |  |
| **E2** |  |  |  |
| A2.1 |  |  |  |
| A2.2 |  |  |  |
| A2.3 |  |  |  |
| **E3** |  |  |  |
| A3.1 |  |  |  |
| A3.2 |  |  |  |
| **E4** |  |  |  |
| A4.1 |  |  |  |
| A4.2 |  |  |  |
| A4.3 |  |  |  |

|  |  |
| --- | --- |
| **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**

1. Chaque entité responsable doit mettre en œuvre un ou plusieurs plans d’intervention en cas d’*incident de cybersécurité* documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-008-6) – Caractéristiques du plan d’intervention en cas d’*incident de cybersécurité*.

*[Facteur de risque de la non-conformité : faible] [Horizon : planification à long terme]*

1. Les pièces justificatives doivent comprendre chacun des plans documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-008-6) – Caractéristiques du plan d’intervention en cas d’*incident de cybersécurité*.

**E1 Alinéa 1.1**

| **Tableau E1 (CIP-008-6) – Caractéristiques du plan d’intervention en cas d’*incident* *de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.1 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Un ou plusieurs processus visant à détecter les *incidents de cybersécurité*, à les classer et à y répondre. | Exemple non limitatif de pièce justificative : plan ou plans d’intervention en cas d’*incident de cybersécurité* documentés et datés qui prévoient un ou des processus pour détecter les *incidents de cybersécurité*, les classer et y répondre. |

**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-008-6, E1, alinéa 1.1**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs plans d’intervention en cas d’*incident de cybersécurité* qui comprennent un ou plusieurs processus visant à détecter les *incidents de cybersécurité*, à les classer et à y répondre. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E1 Alinéa 1.2**

| **Tableau E1 (CIP-008-6) – Caractéristiques du plan d’intervention en cas d’*incident* *de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.2 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Un ou plusieurs processus :  1.2.1 qui comprennent des critères d’évaluation servant à reconnaître les tentatives de compromission ;  1.2.2 qui visent à déterminer si un *incident de cybersécurité* constaté est :   * un *incident de cybersécurité à signaler*; ou * une tentative de compromettre, selon les critères prescrits à l’alinéa 1.2.1, un ou plusieurs systèmes indiqués à la colonne « Systèmes visés » du présent alinéa ; et   1.2.3 qui spécifient une notification selon l’exigence E4. | Exemples non limitatifs de pièces justificatives : plan ou plans d’intervention pour *incident de cybersécurité* documentés et datés qui fournissent des indications ou des seuils pour déterminer quels *incidents de cybersécurité* sont aussi un *incident de cybersécurité à signaler* ou un *incident de cybersécurité* dont on détermine qu’il constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés », y compris la justification des critères d’évaluation, ainsi que des processus documentés de notification. |

**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-008-6, E1, alinéa 1.2**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs plans d’intervention en cas d’*incident de cybersécurité* qui comprennent un ou plusieurs processus avec des critères d’évaluation servant à reconnaître les tentatives de compromission. |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs plans d’intervention en cas d’*incident de cybersécurité* qui comprennent un ou plusieurs processus qui visent à déterminer si un *incident de cybersécurité* constaté est :   * un *incident de cybersécurité à signaler*; ou * une tentative de compromettre, selon les critères prescrits à l’alinéa 1.2.1, un ou plusieurs systèmes indiqués à la colonne « Systèmes visés » du présent alinéa. |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs plans d’intervention en cas d’*incident de cybersécurité* qui comprennent un ou plusieurs processus qui spécifient une notification selon l’exigence E4. |
| **Notes pour l’auditeur:** Si la loi interdit à l’entité responsable de déclarer à l’E-ISAC, alors le processus ne doit pas inclure une disposition de déclarer à l’E-ISAC. Si cette disposition est invoquée, l’équipe d’audit doit vérifier que la loi interdit à l’entité responsable de déclarer à l’E-ISAC. | |

**Notes des auditeurs:**

**E1 Alinéa 1.3**

| **Tableau E1 (CIP-008-6) – Caractéristiques du plan d’intervention en cas d’*incident* *de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.3 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Rôles et responsabilités des groupes ou des personnes chargés de l’intervention en cas d’*incident de cybersécurité*. | Exemple non limitatif de pièce justificative : processus ou procédures d’intervention en cas d’*incident de cybersécurité* datés qui définissent les rôles et les responsabilités (p. ex., surveillance, déclaration, déclenchement, documentation, etc.) des groupes ou des personnes chargés de l’intervention en cas d’*incident de cybersécurité*. |

**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-008-6, E1, alinéa 1.3**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs plans d’intervention en cas d’*incident de cybersécurité* qui définissent les rôles et les responsabilités des groupes ou des personnes chargés de l’intervention en cas d’*incident de cybersécurité*. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E1 Alinéa 1.4**

| **Tableau E1 (CIP-008-6) – Caractéristiques du plan d’intervention en cas d’*incident* *de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.4 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés | Procédures de gestion des *incidents de cybersécurité*. | Exemples non limitatifs de pièces justificatives : processus ou procédures d’intervention en cas d’*incident de cybersécurité* datés qui traitent de la gestion des incidents (p. ex., confinement, élimination, reprise après incident ou résolution de l’incident). |

**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-008-6, E1, alinéa 1.4**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a documenté un ou plusieurs plans d’intervention en cas d’*incident de cybersécurité* qui comprennent les procédures de gestion des *incidents de cybersécurité*. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

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

1. Chaque entité responsable doit mettre en œuvre chacun de ses plans d’intervention en cas d’*incident de cybersécurité* documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d’intervention en cas d’*incident de cybersécurité*.

*[Facteur de risque de non-conformité : faible] [Horizon : planification de l’exploitation et exploitation en temps réel].*

1. Les pièces justificatives doivent comprendre, sans toutefois s’y limiter, des documents qui, collectivement, démontrent la mise en œuvre de tous les alinéas applicables du tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d’intervention en cas d’*incident de cybersécurité*.

**E2 Alinéa 2.1**

| **Tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d’intervention en cas d’*incident de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.1 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Tester chaque plan d’intervention en cas d’*incident de cybersécurité* au moins une fois tous les 15 mois civils :   * en répondant à un *incident de cybersécurité à déclarer* réel ; * en effectuant un exercice de réponse à un *incident de cybersécurité à déclarer*, sur papier ou en salle ; ou * en effectuant un exercice opérationnel de réponse à un *incident de cybersécurité à déclarer*. | Exemple non limitatif de pièce justificative : preuve datée de l’existence d’un rapport sur les leçons apprises qui contient un résumé de l’épreuve ou une compilation des notes, des journaux et des communications qui résultent du test. Les types d’exercices peuvent inclure des exercices axés sur les discussions ou sur les opérations. |

**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-008-6, E2, alinéa 2.1**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a testé chaque plan d’intervention en cas d’*incident de cybersécurité* au moins une fois tous les 15 mois civils :   * en répondant à un *incident de cybersécurité à déclarer* réel ; * en effectuant un exercice de réponse à un *incident de cybersécurité à déclarer*, sur papier ou en salle ; ou * en effectuant un exercice opérationnel de réponse à un *incident de cybersécurité à déclarer*. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E2 Alinéa 2.2**

| **Tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d’intervention en cas d’*incident de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.2 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Utiliser le ou les plans d’intervention en cas d’*incident de cybersécurité* cités à l’exigence E1 au moment de répondre à un *incident de cybersécurité à déclarer*, de répondre à un *incident de cybersécurité* consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa ou d’effectuer un exercice de réponse à un *incident de cybersécurité à déclarer*. Documenter les écarts entre le ou les plans et les mesures prises pendant l’intervention à la suite de l’incident ou lors de l’exercice. | Exemples non limitatifs de pièces justificatives : rapports d’incident, journaux et notes prises durant l’intervention à la suite de l’incident, et documents de suivi décrivant les écarts entre le ou les plans et les mesures prises durant l’intervention à la suite de l’incident ou lors de l’exercice. |

**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-008-6, E2, alinéa 2.2**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a utilisé le ou les plans d’intervention en cas d’*incident de cybersécurité* cités à l’exigence E1 au moment de répondre à un *incident de cybersécurité à déclarer*, de répondre à un *incident de cybersécurité* consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa ou d’effectuer un exercice de réponse à un *incident de cybersécurité à déclarer*. |
|  | Vérifier que l’entité responsable a documenté les écarts entre le ou les plans, s’il y en a, et les mesures prises pendant l’intervention à la suite de l’*incident* *de cybersécurité à déclarer* ou lors d’un *incident de cybersécurité* consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa, ou au moment d’effectuer un exercice de réponse à un *incident de cybersécurité à déclarer*. |
| **Notes pour l’auditeur:**  La pratique de la réponse à un incident nécessite la capacité d’être flexible au moment de répondre à des *incidents de cybersécurité*. Ceci est reconnu par la disposition du présent alinéa relative à la documentation des écarts par rapport au plan d’intervention en cas d’incidents de l’entité responsable. L’auditeur doit noter que, bien que des écarts par rapport au plan d’intervention en cas d’incidents soient autorisés, les écarts par rapport au libellé de l’exigence (vérification du plan au moins une fois tous les 15 mois civils, notification à l’E-ISAC des incidents applicables, etc.), ne sont pas permis. | |

**Notes des auditeurs:**

**E2 Alinéa 2.3**

| **Tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d’intervention en cas d’*incident de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.3 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Conserver les dossiers relatifs aux *incidents de cybersécurité à déclarer* et aux *incidents de cybersécurité* consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa conformément aux plans d’intervention en cas d’*incident de cybersécurité* spécifiés à l’exigence E1. | Exemples non limitatifs de pièces justificatives : documents datés, tels que journaux de sécurité, rapports de police, courriels, formulaires d’intervention ou listes de contrôle, résultats d’analyses judiciaires, dossiers de remise en charge et notes d’analyse après incident relativement à *des incidents de cybersécurité à déclarer* et à des *incidents de cybersécurité* consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés ». |

**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-008-6, E2, alinéa 2.3**

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

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a conservé les dossiers relatifs aux *incidents de cybersécurité à déclarer* et aux *incidents de cybersécurité* consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa conformément aux plans d’intervention en cas d’*incident de cybersécurité* spécifiés à l’exigence E1. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

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

1. Chaque entité responsable doit tenir à jour chacun de ses plans d’intervention en cas d’*incident de cybersécurité* conformément à chacun des alinéas applicables du tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d’intervention en cas d’*incident de cybersécurité*.

*[Facteur de risque de non-conformité : faible] [Horizon : évaluation de activités d’exploitation]*

1. Les pièces justificatives doivent comprendre, sans toutefois s’y limiter, des documents qui, collectivement, démontrent que tous les plans d’intervention en cas d’*incident de cybersécurité* sont tenus à jour conformément aux alinéas applicables du tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d’intervention en cas d’*incident de cybersécurité*.

**E3 Alinéa 3.1**

| **Tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d’intervention en cas d’*incident de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.1 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Au plus tard 90 jours civils après la réalisation d’un test des plans d’intervention en cas d’*incident de cybersécurité* ou après une intervention réelle en cas d’*incident de cybersécurité à déclarer*:   * + 1. documenter les leçons apprises, ou encore l’absence de leçons apprises ;     2. mettre à jour le plan d’intervention en cas d’*incident de cybersécurité* en tenant compte des leçons apprises documentées qui se rapportent à ce plan ; et     3. aviser chaque personne ou groupe qui joue un rôle défini dans le plan d’intervention en cas d’*incident de cybersécurité* des mises à jour à ce plan qui tiennent compte des leçons apprises documentées. | Exemples non limitatifs de pièces justificatives :   1. documents datés, tels que notes de réunion après incident ou rapports de suivi indiquant les leçons apprises associées à la mise à l’épreuve du ou des plans d’intervention en cas d’*incident de cybersécurité* ou à une intervention réelle en cas d’*incident de cybersécurité à déclarer*, ou encore documents datés confirmant l’absence de leçons apprises ; 2. plan d’intervention en cas d’*incident de cybersécurité* daté et révisé indiquant toutes les modifications apportées en tenant compte des leçons apprises ; et 3. preuve de distribution du plan révisé, par exemple :    * courriels ;    * service postal (US Postal Service ou autre) ;    * système de distribution électronique ; ou    * feuilles de présence aux formations. |

**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-008-6, E3, alinéa 3.1**

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

|  |  |
| --- | --- |
|  | Vérifier qu’au plus tard 90 jours civils après la réalisation d’un test des plans d’intervention en cas d’*incident de cybersécurité* ou après une intervention réelle en cas d’*incident de cybersécurité à déclarer*, l’entité responsable a :   1. documenté les leçons apprises, ou encore l’absence de leçons apprises ; 2. mis à jour le plan d’intervention pour *incident de cybersécurité* en tenant compte des leçons apprises documentées qui se rapportent à ce plan ; et 3. avisé chaque personne ou groupe qui joue un rôle défini dans le plan d’intervention en cas d’*incident de cybersécurité* des mises à jour à ce plan qui tiennent compte des leçons apprises documentées. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E3 Alinéa 3.2**

| **Tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d’intervention en cas d’*incident de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.2 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Au plus tard 60 jours civils après qu’un changement jugé par l’entité responsable comme ayant un impact sur la capacité d’exécuter le plan a été apporté aux rôles ou responsabilités, aux groupes ou personnes chargés de l’intervention en cas d’*incident de cybersécurité* ou à une technologie :   * + 1. mettre à jour le ou les plans d’intervention en cas d’*incident de cybersécurité*; et     2. aviser des mises à jour chaque personne ou groupe jouant un rôle défini dans le plan d’intervention en cas d’*incident de cybersécurité*. | Exemples non limitatifs de pièces justificatives :   1. plan d’intervention en cas d’*incident de cybersécurité* révisé et daté comprenant les changements apportés aux rôles ou responsabilités, aux intervenants ou à une technologie ; et 2. preuve de distribution du plan révisé, par exemple :    * courriels ;    * service postal (US Postal Service ou autre) ;    * système de distribution électronique ; ou    * feuilles de présence aux formations. |

**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-008-6, E3, alinéa 3.2**

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

|  |  |
| --- | --- |
|  | Vérifier qu’au plus tard 60 jours civils après qu’un changement jugé par l’entité responsable comme ayant un impact sur la capacité d’exécuter le plan a été apporté aux rôles ou responsabilités, aux groupes ou personnes chargés de l’intervention en cas d’*incident de cybersécurité* ou à une technologie, l’entité responsable a :   1. mis à jour le ou les plans d’intervention en cas d’*incident de cybersécurité* ; et 2. avisé des mises à jour chaque personne ou groupe jouant un rôle défini dans le plan d’intervention en cas d’*incident de cybersécurité*. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

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

1. Chaque entité responsable doit aviser l’Electricity Information Sharing and Analysis Center (E-ISAC) et aussi, si elle est soumise à la réglementation des États-Unis, le National Cybersecurity and Communications Integration Center (NCCIC)[[2]](#footnote-2) des États-Unis, ou leurs remplaçants éventuels, de tout *incident de cybersécurité à déclarer* et de tout *incident de cybersécurité* qui constitue une tentative de compromettre, selon les critères prescrits à l’alinéa 1.2.1 de l’exigence E1, un système indiqué à la colonne « Systèmes visés », à moins que la loi ne l’interdise, conformément à chacun des alinéas applicables du tableau E4 (CIP-008-6) – Notification et déclaration des *incidents de cybersécurité*.

*[Facteur de risque de non-conformité : faible] [Horizon : évaluation de activités d’exploitation]*

1. Les pièces justificatives doivent comprendre, sans toutefois s’y limiter, des documents qui, collectivement, démontrent la notification de chaque *incident de cybersécurité à déclarer* et *incident de cybersécurité* qui constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés », conformément aux alinéas applicables du tableau E4 (CIP-008-6) – Notification et déclaration des *incidents de cybersécurité*.

**E4 Alinéa 4.1**

| **Tableau E4 (CIP-008-6) – Notification et déclaration des *incidents de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.1 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Les notifications initiales et leurs mises à jour doivent au minimum préciser les éléments suivants, dans la mesure où ils sont connus :  4.1.1 l’impact fonctionnel ;  4.1.2 le vecteur d’attaque utilisé ; et  4.1.3 le degré d’intrusion atteint ou visé. | Exemples non limitatifs de pièces justificatives : documents datés de notification initiale et de mise à jour transmis à l’E-ISAC et au NCCIC. |

**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-008-6, E4, alinéa 4.1**

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

|  |  |
| --- | --- |
|  | Vérifier que les notifications initiales et leurs mises à jour précisaient les éléments suivants, dans la mesure où ils sont connus :   1. l’impact fonctionnel ; 2. le vecteur d’attaque utilisé ; et 3. le degré d’intrusion atteint ou visé. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E4 Alinéa 4.2**

| **Tableau E4 (CIP-008-6) – Notification et déclaration des *incidents de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.2 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Après la détermination par l’entité responsable selon le ou les processus documentés prescrits à l’alinéa 1.2 de l’exigence E1, transmettre une notification initiale dans les délais suivants :   * une heure après avoir déterminé qu’il s’est produit un *incident de cybersécurité à signaler* ; * au plus tard à la fin du jour civil suivant la détermination qu’un *incident de cybersécurité* constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa. | Exemples non limitatifs de pièces justificatives : documents datés de notification transmis à l’E-ISAC et au NCCIC. |

**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-008-6, E4, alinéa 4.2**

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

|  |  |
| --- | --- |
|  | Pour chaque *incident de cybersécurité à signaler* tel que déterminé selon le ou les processus documentés prescrits à l’alinéa 1.2 de l’exigence E1, vérifier que la notification initiale a été transmise à chaque organisme applicable dans le délai d’une heure après avoir déterminé qu’il s’est produit un *incident de cybersécurité à signaler*. |
|  | Pour chaque *incident de cybersécurité* qui constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa et déterminé selon le ou les processus documentés prescrits à l’alinéa 1.2 de l’exigence E1, vérifier que la notification initiale a été transmise à chaque organisme applicable au plus tard à la fin du jour civil suivant la détermination qu’un *incident de cybersécurité* constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**E4 Alinéa 4.3**

| **Tableau E4 (CIP-008-6) – Notification et déclaration des *incidents de cybersécurité*** | | | |
| --- | --- | --- | --- |
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 4.3 | *Systèmes électroniques BES* à impact élevé et :   * les *EACMS* associés.   *Systèmes électroniques BES* à impact moyen et :   * les *EACMS* associés. | Transmettre toute mise à jour pertinente, dans un délai de 7 jours civils après avoir déterminé des ajouts ou des changements aux éléments d’information exigés à l’alinéa 4.1. | Exemples non limitatifs de pièces justificatives : documents datés transmis à l’E-ISAC et au NCCIC. |

**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-008-6, E4, alinéa 4.3**

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

|  |  |
| --- | --- |
|  | Pour chaque *incident de cybersécurité à signaler* et chaque *incident de cybersécurité* qui constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa, vérifier que les mises à jour pertinentes ont été transmises dans un délai de 7 jours civils après avoir déterminé des ajouts ou des changements aux éléments d’information. |
| **Notes pour l’auditeur:** | |

**Notes des auditeurs:**

**Information supplémentaire**

**Norme de fiabilité**

Le texte complet de la norme CIP-008-6 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 | Octobre 2022 | Document initial | Document créé à partir du formulaire « RSAW » de la NERC |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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)
2. Le National Cybersecurity and Communications Integration Center (NCCIC) est l’organisme qui remplace l’Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). En 2017, le NCCIC a réorganisé ses structures en y intégrant des fonctions antérieurement remplies de façon indépendante par l’ICS-CERT et par la United States Computer Emergency Readiness Team (US-CERT). [↑](#footnote-ref-2)