

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-010-34 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

La présente annexe établit les dispositions particulières d'application au Québec de la norme qu'elle vise. Les dispositions de la norme visée et de l'annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe a préséance.

A. Introduction

1. **Titre :** Aucune disposition particulière.
2. **Numéro :** Aucune disposition particulière.
3. **Objet :** Aucune disposition particulière.
4. **Applicabilité :**

4.1. Entités fonctionnelles

Aucune disposition particulière.

4.2. Installations

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

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

- Toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'installation est de 300 MVA ou moins et (2) aucun groupe de l'installation ne peut être synchronisé avec un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. Date d'entrée en vigueur :

- | | |
|--|--------------|
| 5.1. Adoption de la norme par la Régie de l'énergie : | xx mois 20xx |
| 5.2. Adoption de l'annexe par la Régie de l'énergie : | xx mois 20xx |
| 5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : | xx mois 20xx |

6. Contexte : Aucune disposition particulière.

B. Exigences et mesures

Aucune disposition particulière.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-010-34 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

Au Québec, le terme *responsable des mesures pour assurer la conformité* désigne la Régie de l'énergie dans le rôle visant à surveiller la conformité avec la norme de fiabilité visée et à la présente annexe, et à assurer l'application de celles-ci.

1.2. Conservation des pièces justificatives

Aucune disposition particulière.

1.3. Programme de surveillance de la conformité et d'application des normes

La Régie de l'énergie établit les processus de surveillance qui servent à évaluer les données ou l'information afin de déterminer la conformité ou la non-conformité avec la norme de fiabilité visée et avec la présente annexe.

Niveau de gravité de la non-conformité (VSL)

Aucune disposition particulière.

~~Correction de l'erratum pour le VSL modéré de l'exigence E3, ajout « et moins de 21 mois » dans la partie suivante de la phrase « a effectué une analyse de vulnérabilité dans un délai de plus de 18 mois et de moins de 21 mois suivant la dernière analyse de l'un de ses systèmes.~~

Ex.#	VSL faible	VSL modéré	VSL élevé	VSL critique
E3.	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 15 mois et de moins de 18 mois suivant la dernière analyse de l'un de ses systèmes électroniques BES visés. (3.1) OU L'entité responsable a mis en œuvre un ou	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 18 mois et de moins de 21 mois suivant la dernière analyse de l'un de ses systèmes électroniques BES visés. (3.1) OU L'entité responsable a mis en œuvre un ou	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 21 mois et de moins de 24 mois suivant la dernière analyse de l'un de ses systèmes électroniques BES visés. (3.1) OU L'entité responsable a mis en œuvre un ou	L'entité responsable n'a mis en œuvre aucun processus d'analyse de vulnérabilité pour un de ses systèmes électroniques BES visés. (E3) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle a effectué une analyse de vulnérabilité plus de 24 mois suivant la

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-010-34 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

	plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 36 mois et de moins de 39 mois suivant la dernière analyse active de l'un de ses systèmes électroniques BES visés. (3.2)	plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 39 mois et de moins de 42 mois suivant la dernière analyse active de l'un de ses systèmes électroniques BES visés. (3.2)	plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 42 mois et de moins de 45 mois suivant la dernière analyse active de l'un de ses systèmes électroniques BES visés. (3.2)	<p>dernière analyse de l'un de ses systèmes électroniques BES visés. (3.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 45 mois suivant la dernière analyse active de l'un de ses systèmes électroniques BES visés. (3.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre et documenté un ou plusieurs processus d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle n'a pas effectué l'analyse de vulnérabilité active d'une manière qui simule une configuration de référence existante de ses systèmes électroniques BES visés. (3.3)</p>
--	--	--	--	---

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-010-34 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

				OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle n'a pas documenté les résultats des analyses de vulnérabilité, les plans d'action pour corriger ou atténuer les vulnérabilités constatées dans les analyses, la date planifiée d'achèvement du plan d'action et l'état d'exécution des plans d'atténuation. (3.4)
--	--	--	--	--

D. Différences régionales

Aucune disposition particulière.

E. Documents connexes

Aucune disposition particulière.

CIP-010-4 – Annexe 1

Aucune disposition particulière.

CIP-010-4 – Annexe 2

Aucune disposition particulière

Principes directeurs et fondements techniques

~~Aucune disposition particulière.~~

Historique des révisions

Version	Date	Intervention	Suivi des modifications
---------	------	--------------	-------------------------

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-010-~~34~~ – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

1	xx mois 20xx	Nouvelle annexe <u>en suivi de la décision D- xxxx-yyy.</u>	Nouvelle
---	--------------	---	----------