

**TABLE OF CONTENTS**

**TABLE DES MATIÈRES**

**A. INTRODUCTION**

- 1. Title
- 2. Number
- 3. Purpose
- 4. Applicability
- 5. Effective Date

**B. REQUIREMENTS**

R1 to R5

**C. MEASURES**

M1 to M5

**D. COMPLIANCE**

- 1. Compliance Monitoring Process
  - 1.1 Compliance Monitoring Responsibility
  - 1.2 Compliance Monitoring Period and Reset Time Frame
  - 1.3 Data Retention
  - 1.4 Additional Compliance Information
- 2. Levels of Non-Compliance
  - 2.1 Level 1
  - 2.2 Level 2
  - 2.3 Level 3
  - 2.4 Level 4

**E. REGIONAL DIFFERENCES**

**VERSION HISTORY**

**A. INTRODUCTION**

- 1. Titre
- 2. Numéro
- 3. Objet
- 4. Applicabilité
- 5. Date d'entrée en vigueur

**B. EXIGENCES**

E1 à E4

**C. MESURES**

M1 à M4

**D. CONFORMITÉ**

- 1. Processus de vérification de la conformité
  - 1.1 Responsabilité de la vérification de la conformité
  - 1.2 Période de vérification de la conformité et délai de retour en conformité
  - 1.3 Conservation des données
  - 1.4 Autre information sur la conformité
- 2. Niveaux de non-conformité
  - 2.1 Niveau 1
  - 2.2 Niveau 2
  - 2.3 Niveau 3
  - 2.4 Niveau 4

**E. DIFFÉRENCES RÉGIONALES**

**HISTORIQUE DES VERSIONS**

Ch.	English version		Version française
-----	-----------------	--	-------------------

**A. Introduction / Introduction**

1.	<b>Title:</b> Cyber Security — Personnel & Training	1.	<b>Titre :</b> Cybersécurité — Personnel et formation
2.	<b>Number:</b> CIP-004-1	2.	<b>Numéro :</b> CIP-004-1
3.	<b>Purpose:</b> Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.	3.	<b>Objet :</b> La norme CIP-004 exige des employés ainsi que des entrepreneurs et des fournisseurs ayant un accès électronique ou physique autorisé sans escorte aux actifs électroniques critiques que leur niveau d'autorisation concorde avec l'évaluation des risques liés au personnel <sup>(*)</sup> et qu'ils détiennent une formation et une sensibilisation à la sécurité adéquates.  <small>(*) L'évaluation des risques liés au personnel désigne en pratique la vérification des antécédents.</small>
	Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.		La norme CIP-004 fait partie du groupe de normes CIP-002 à CIP-009 et doit être lue dans ce contexte. Les entités responsables doivent interpréter et mettre en pratique les normes CIP-002 à CIP-009 tout en tenant raisonnablement compte des impératifs d'affaires qui s'imposent.
4.	<b>Applicability:</b>	4	<b>Applicabilité :</b>
4.1	Within the text of Standard CIP-004, "Responsible Entity" shall mean :	4.1	Dans le contexte de la norme CIP-004, l'expression « entité responsable » désigne :
4.1.1	Reliability Coordinator.	4.1.1	Coordonnateur de la fiabilité
4.1.2	Balancing Authority.	4.1.2	Responsable de l'équilibrage
4.1.3	Interchange Authority.	4.1.3	Responsable des échanges
4.1.4	Transmission Service Provider.	4.1.4	Fournisseur de services de transport
4.1.5	Transmission Owner.	4.1.5	Propriétaire du réseau de transport
4.1.6	Transmission Operator.	4.1.6	Exploitant du réseau de transport
4.1.7	Generator Owner.	4.1.7	Propriétaire d'installations de production
4.1.8	Generator Operator.	4.1.8	Exploitant d'installations de production
4.1.9	Load Serving Entity.	4.1.9	Responsable de l'approvisionnement
4.1.10	NERC.	4.1.10	NERC.

Ch.	English version		Version française
4.1.11	Regional Reliability Organizations.	4.1.11	Organisations régionales de fiabilité
4.2	The following are exempt from Standard CIP-004 :	4.2	Les entités suivantes sont exemptées de la norme CIP-004 :
4.2.1	Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.	4.2.1	Les installations réglementées par la <i>U.S. Nuclear Regulatory Commission</i> ou la Commission canadienne de sûreté nucléaire.
4.2.2	Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.	4.2.2	Les actifs électroniques associés aux réseaux de communication et aux liaisons de communication entre les périmètres de sécurité électroniques discrets.
4.2.3	Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.	4.2.3	Les entités responsables qui, en conformité avec la norme CIP-002, ont indiqué qu'elles ne détiennent aucun actif électronique critique.
5.	<b>Effective Date:</b> June 1, 2006.	5	<b>Date d'entrée en vigueur :</b> 1 <sup>er</sup> juin 2006.

## B. Requirements / Exigences

R1	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:	E1	Sensibilisation — L'entité responsable doit mettre en place, gérer, et documenter un programme de sensibilisation à la sécurité pour s'assurer que le personnel ayant un accès électronique ou physique autorisé sans escorte reçoive un rappel périodique des bonnes pratiques de sécurité. Le programme doit inclure un rappel de sensibilisation au moins à tous les trois mois à l'aide de :
	<ul style="list-style-type: none"> <li>• Direct communications (e.g., emails, memos, computer based training, etc.);</li> </ul>		<ul style="list-style-type: none"> <li>• communications directes (p. ex., courriels, mémos, présentations informatiques, etc.)</li> </ul>
	<ul style="list-style-type: none"> <li>• Indirect communications (e.g., posters, intranet, brochures, etc.);</li> </ul>		<ul style="list-style-type: none"> <li>• communications indirectes (p. ex., affiches, intranet, brochures, etc.)</li> </ul>
	<ul style="list-style-type: none"> <li>• Management support and reinforcement (e.g., presentations, meetings, etc.).</li> </ul>		<ul style="list-style-type: none"> <li>• renforcement et de soutien de la part des gestionnaires (p. ex., présentations, réunions, etc.)</li> </ul>
R2	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	E2	Formation — L'entité responsable doit établir, gérer et documenter un programme annuel de formation sur la cybersécurité pour son personnel ayant un accès électronique ou physique autorisé sans escorte. Ce programme doit être revu annuellement et mis à jour au besoin.

Ch.	English version		Version française
R2.1	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.	E2.1	Ce programme permettra de s'assurer que tous les employés ayant accès aux actifs électroniques critiques, y compris les entrepreneurs et les fournisseurs de services, sont formés dans les 90 jours civils suivant l'octroi du privilège d'accès.
R2.2	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	E2.2	La formation doit porter sur les politiques, les contrôles d'accès et les procédures mis au point pour les actifs électroniques critiques décrits dans la norme CIP-004, et inclure, au moins, les exigences suivantes selon les rôles et responsabilités du personnel :
R2.2.1	The proper use of Critical Cyber Assets;	E2.2.1	la bonne façon d'utiliser les actifs électroniques critiques,
R2.2.2	Physical and electronic access controls to Critical Cyber Assets;	E2.2.2	les contrôles physiques et électroniques d'accès aux actifs électroniques critiques,
R2.2.3	The proper handling of Critical Cyber Asset information; and,	E2.2.3	la gestion adéquate des renseignements sur les actifs électroniques critiques,
R2.2.4	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	E2.2.4	les plans d'action et les procédures pour la récupération ou la réinitialisation des actifs électroniques critiques et de leurs accès après un cyberincident de sécurité.
R2.3	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	E2.3	L'entité responsable doit conserver une preuve documentaire qui atteste que la formation est donnée au moins une fois l'an, incluant les dates de présentation de la formation ainsi que la liste des participants.
R3	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	E3	Évaluation des risques liés au personnel — L'entité responsable doit documenter un programme d'évaluation des risques liés au personnel en conformité avec les lois fédérales, provinciales, municipales, et avec les ententes syndicales en vigueur, à l'intention des employés ayant un accès électronique ou physique autorisé sans escorte,. Une évaluation des risques liés au personnel doit être effectuée conformément au programme dans les 30 jours suivant l'octroi du privilège d'accès. Ce programme doit minimalement inclure les aspects suivants :
R3.1	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	E3.1	L'entité responsable doit s'assurer que chaque évaluation inclut, au moins, la vérification de l'identité (p. ex., le numéro d'assurance sociale) et la vérification judiciaire portant sur les sept dernières années. Dans la mesure permise par la loi et sous réserve d'ententes syndicales existantes, l'entité responsable peut faire d'autres vérifications selon la criticité du poste occupé.

Ch.	English version		Version française
R3.2	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	E3.2	L'entité responsable doit faire la mise à jour de l'évaluation des risques liés au personnel au moins tous les sept ans après la première analyse ou pour un motif valable.
R3.3	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.	E3.3	L'entité responsable doit documenter les résultats de l'évaluation des risques liés à son personnel ayant un accès électronique ou physique autorisé sans escorte, incluant les entrepreneurs et les fournisseurs de services, conformément à la norme CIP-004.
R4	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	E4	Accès — L'entité responsable doit maintenir la ou les listes des employés ayant un accès électronique ou physique autorisé sans escorte, incluant leurs propres privilèges d'accès électronique ou physique aux actifs électroniques critiques.
R4.1	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	E4.1	L'entité responsable doit revoir la ou les listes du personnel ayant accès aux actifs électroniques critiques à tous les trois mois et mettre à jour les listes dans les sept jours suivant tout changement de personnel ou de ses privilèges d'accès. L'entité responsable doit s'assurer que la ou les listes des entrepreneurs et des fournisseurs de services sont correctement mises à jour.
R4.2	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	E4.2	L'entité responsable doit révoquer l'accès aux actifs électroniques critiques dans les 24 heures dans le cas d'un licenciement motivé d'un membre du personnel et dans les sept jours civils pour un membre du personnel qui n'est plus tenu d'avoir accès à ces actifs électroniques critiques.

### C. Measures / Mesures

	The following measures will be used to demonstrate compliance with the requirements of Standard CIP-004:		Les mesures suivantes serviront à établir la preuve de la conformité aux exigences de la norme CIP-004 :
M1	Documentation of the Responsible Entity's security awareness and reinforcement program as specified in Requirement R1.	M1	La documentation sur le programme de sensibilisation et de renforcement de l'entité responsable conformément à l'exigence E1.
M2	Documentation of the Responsible Entity's cyber security training program, review, and records as specified in Requirement R2.	M2	La documentation sur le programme de formation, sur la vérification et sur les dossiers relatifs à la cybersécurité de l'entité responsable conformément à l'exigence E2.

Ch.	English version		Version française
M3	Documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.	M3	La documentation sur le programme d'évaluation des risques liés au personnel et les éléments de preuve qui attestent que le programme a été mis en œuvre pour tout le personnel ayant un accès électronique ou physique sans escorte à des actifs électroniques critiques conformément à l'exigence E3.
M4	Documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.	M4	La documentation sur les listes, sur leur vérification et sur leur mise à jour et, au besoin, sur la révocation d'accès conformément à l'exigence E4.

#### D. Compliance / Conformité

1.	<b>Compliance Monitoring Process</b>	1.	<b>Processus de vérification de la conformité</b>
1.1	<b>Compliance Monitoring Responsibility</b>	1.1	<b>Responsabilité de la vérification de la conformité</b>
1.1.1	Regional Reliability Organizations for Responsible Entities.	1.1.1	Les organisations régionales de fiabilité pour les entités responsables.
1.1.2	NERC for Regional Reliability Organization.	1.1.2	La NERC pour les organisations régionales de fiabilité.
1.1.3	Third-party monitor without vested interest in the outcome for NERC.	1.1.3	Un vérificateur tiers n'ayant pas d'intérêt quant aux résultats pour la NERC.
1.2	<b>Compliance Monitoring Period and Reset Time Frame</b> Annually.	1.2	<b>Période de vérification de la conformité et délai de retour en conformité</b> Annuelle
1.3	<b>Data Retention</b>	1.3	<b>Conservation des données</b>
1.3.1	The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.	1.3.1	L'entité responsable doit conserver la documentation sur l'évaluation des risques liés au personnel en accord avec les lois fédérales, provinciales et municipales.
1.3.2	The Responsible Entity shall keep other documents and records required by Standard CIP-004 from the previous full calendar year.	1.3.2	L'entité responsable doit conserver toute la documentation requise en vertu de la norme CIP-004 pour la dernière année civile.
1.3.3	The compliance monitor shall keep audit records for three years.	1.3.3	Le vérificateur de la conformité doit garder les dossiers d'audit des trois dernières années.
1.4	<b>Additional Compliance Information</b>	1.4	<b>Autre information sur la conformité</b>
1.4.1	Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.	1.4.1	L'entité responsable doit faire la preuve de sa conformité au moyen d'une autocertification ou d'une vérification, selon ce que déterminera le vérificateur de la conformité.

Ch.	English version		Version française
1.4.2	Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.	1.4.2	Les cas où l'entité responsable n'est pas conforme à sa politique de cybersécurité doivent être documentés et approuvés par le cadre supérieur désigné ou son ou ses délégués. Se reporter à l'exigence E3 de la norme CIP-003. Les exceptions dûment autorisées ne conduiront pas à une non-conformité.
2.	<b>Levels of Non-Compliance</b>	2.	<b>Niveaux de non-conformité</b>
2.1	<b>Level 1:</b>	2.1	<b>Niveau 1 :</b>
2.1.1	Awareness program exists, but is not conducted within the minimum required period of quarterly reinforcement; or,	2.1.1	Le programme de sensibilisation existe, mais il n'a pas été mené selon les exigences d'une période trimestrielle minimale de renforcement; ou,
2.1.2	Training program exists, but records of training either do not exist or reveal that personnel who have access to Critical Cyber Assets were not trained as required; or,	2.1.2	La formation existe, mais les dossiers de formation n'existent pas ou révèlent que des employés ayant accès à des actifs électroniques critiques n'ont pas été formés comme prévu; ou,
2.1.3	Personnel risk assessment program exists, but documentation of that program does not exist; or,	2.1.3	Le programme d'évaluation des risques liés au personnel existe, mais la documentation sur le programme n'existe pas; ou,
2.1.4	List(s) of personnel with their access rights is available, but has not been reviewed and updated as required.	2.1.4	Les listes des membres du personnel et de leurs droits d'accès sont disponibles, mais elles n'ont pas été vérifiées et mises à jour tel qu'exigé.
2.1.5	One personnel risk assessment is not updated at least every seven years, or for cause; or,	2.1.5	Une des analyses des risques liés au personnel n'a pas été mise à jour au moins à tous les sept ans, ou pour un motif déterminé; ou,
2.1.6	One instance of personnel (employee, contractor or service provider) change other than for cause in which access to Critical Cyber Assets was no longer needed was not revoked within seven calendar days.	2.1.6	Une modification au statut d'un membre du personnel (employé, entrepreneur ou fournisseur de services) faisant en sorte qu'il n'a plus accès aux actifs électroniques critiques pour toute autre raison que son licenciement motivé n'a pas été effectuée dans les sept jours suivant la révocation d'accès.
2.2	<b>Level 2:</b>	2.2	<b>Niveau 2 :</b>
2.2.1	Awareness program does not exist or is not implemented; or,	2.2.1	Le programme de sensibilisation n'existe pas ou n'a pas été mis en place; ou,
2.2.2	Training program exists, but does not address the requirements identified in Standard CIP-004; or,	2.2.2	Le programme de formation existe, mais il ne porte pas sur les exigences de la norme CIP-004; ou,
2.2.3	Personnel risk assessment program exists, but assessments are not conducted as required; or,	2.2.3	Le programme d'évaluation des risques liés au personnel existe, mais les vérifications n'ont pas été faites tel qu'exigé; ou,

Ch.	English version		Version française
2.2.4	One instance of personnel termination for cause (employee, contractor or service provider) in which access to Critical Cyber Assets was not revoked within 24 hours.	2.2.4	Un membre du personnel (employé, entrepreneur ou fournisseur de services) a été licencié pour un motif déterminé et ses accès aux actifs électroniques critiques n'ont pas été révoqués dans les 24 heures qui ont suivi.
2.3	<b>Level 3:</b>	2.3	<b>Niveau 3 :</b>
2.3.1	Training program exists, but has not been reviewed and updated at least annually; or,	2.3.1	Le programme de formation existe, mais il n'a pas été revu et mis à jour, au moins une fois par année; ou,
2.3.2	A personnel risk assessment program exists, but records reveal program does not meet the requirements of Standard CIP-004; or,	2.3.2	Un programme d'évaluation des risques liés au personnel existe, mais les dossiers indiquent que le programme n'est pas conforme aux exigences de la norme CIP-004; ou,
2.3.3	List(s) of personnel with their access control rights exists, but does not include service vendors and contractors.	2.3.3	La ou les listes des membres du personnel et de leurs privilèges d'accès existent mais elles ne comprennent pas les entrepreneurs et les fournisseurs de services.
2.4	<b>Level 4:</b>	2.4	<b>Niveau 4 :</b>
2.4.1	No documented training program exists; or,	2.4.1	Aucun programme de formation documenté n'existe; ou,
2.4.2	No documented personnel risk assessment program exists; or,	2.4.2	Aucun programme documenté d'évaluation des risques liés au personnel n'existe; ou,
2.4.3	No required documentation created pursuant to the training or personnel risk assessment programs exists.	2.4.3	Aucune documentation sur le programme de formation ou sur le programme d'évaluation des risques liés au personnel n'existe.

**E. Regional Differences / Différences régionales**

1.	None identified.	1.	Aucune n'a été établie.
----	------------------	----	-------------------------

**Version History**

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase “for cause” as intended. “One instance of personnel termination for cause...”	03/24/06
1	06/01/06	D.2.1.4 — Change “access control rights” to “access rights.”	06/05/06

**Historique des versions**

Version	Date	Intervention	Suivi des modifications
1	16 janvier 2006	D.2.2.4 — Ajout de l’expression « for cause » comme prévu. « One instance of personnel termination for cause... » dans la version anglaise	24 mars 2006
1	1 <sup>er</sup> juin 2006	D.2.1.4 — Remplacer « access control rights » par « access rights » dans la version anglaise	5 juin 2006