

TABLE OF CONTENTS

TABLE DES MATIÈRES

A. INTRODUCTION

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

B. REQUIREMENTS

R1 to R6

C. MEASURES

M1 to M6

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 E6

C. MESURES

M1 à M6

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

Traduction française de la norme de la NERC CIP-003-1

Cyber Security — Security Management Controls

Cybersécurité — Mécanismes de gestion de la sécurité

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

A. Introduction / Introduction

1.	Title: Cyber Security — Security Management Controls	1.	Titre : Cybersécurité — Mécanismes de gestion de la sécurité
2.	Number: CIP-003-1	2.	Numéro : CIP-003-1
3.	Purpose: Norme CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.	3.	Objet : La norme CIP-003 exige des entités responsables qu'elles mettent en place des mécanismes minimaux de gestion de la sécurité dans le but de protéger les actifs électroniques essentiels.
	Norme CIP-003 should be read as part of a group of normes 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-003 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.	Applicability:	4.	Applicabilité :
4.1	Within the text of Standard CIP-003, “Responsible Entity” shall mean:	4.1	Dans le contexte de la norme CIP-003, 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
4.1.11	Regional Reliability Organizations	4.1.11	Organisations régionales de fiabilité

Traduction française de la norme de la NERC CIP-003-1

Cyber Security — Security Management Controls

Cybersécurité — Mécanismes de gestion de la sécurité

Ch.	English Version		Version française
4.2	The following are exempt from Standard CIP-003:	4.2	Les entités suivantes sont exemptées de la norme CIP-003 :
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	L'entité responsable qui, en conformité avec la norme CIP-002, a indiqué qu'elle ne détient aucun actif électronique critiques.
5.	Effective Date: June 1, 2006.	5.	Date d'entrée en vigueur : 1 ^{er} juin 2006

B. Requirements / Exigences

R1	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	E1	Politique de cybersécurité — L'entité responsable doit documenter et mettre en œuvre une politique de cybersécurité qui représente l'engagement de la direction et sa capacité à sécuriser ses actifs électroniques critiques. L'entité responsable doit, au minimum, s'assurer de ce qui suit :
R1.1	The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.	E1.1	La politique de cybersécurité couvre les exigences des normes CIP-002 à CIP-009, y compris les dispositions touchant les cas d'urgence.
R1.2	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	E1.2	La politique de cybersécurité est facilement disponible pour tout le personnel qui a accès aux actifs électroniques essentiels ou qui en est responsable.
R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	E1.3	La révision annuelle et l'approbation de la politique de cybersécurité sont effectuées par le cadre supérieur désigné en vertu de l'exigence E2.
R2	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.	E2	Direction — L'entité responsable doit nommer un cadre supérieur ayant l'entière responsabilité d'assurer la direction et la gestion de la mise en œuvre des normes CIP-002 à CIP-009 et l'adhésion à celles-ci au sein de l'entité.
R2.1	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	E2.1	Les renseignements à consigner sur l'identité du cadre supérieur doivent comprendre son nom, son titre, son numéro de téléphone au travail, son adresse au travail et la date de sa nomination.

Traduction française de la norme de la NERC CIP-003-1

Cyber Security — Security Management Controls

Cybersécurité — Mécanismes de gestion de la sécurité

Ch.	English Version		Version française
R2.2	Changes to the senior manager must be documented within thirty calendar days of the effective date.	E2.2	Les changements concernant l'identité du cadre supérieur doivent être documentés dans les trente (30) jours de la date d'entrée en vigueur.
R2.3	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	E2.3	Le cadre supérieur ou son (ses) délégué(s) doit (doivent) autoriser et documenter toute exception aux exigences de la politique de cybersécurité.
R3	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	E3	Exceptions — Dans les cas où l'entité responsable ne peut agir conformément à sa politique de cybersécurité, les exceptions doivent être documentées et autorisées par le cadre supérieur ou son (ses) délégué(s).
R3.1	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	E3.1	Les exceptions à la politique de cybersécurité de l'entité responsable doivent être documentées dans les trente (30) jours suivant leur approbation par le cadre supérieur ou son (ses) délégué(s).
R3.2	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.	E3.2	La documentation des exceptions à la politique de cybersécurité doit comprendre une justification écrite de la nécessité de l'exception et toutes les mesures compensatoires ou une déclaration d'acceptation des risques.
R3.3	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	E3.3	Les exceptions autorisées à la politique de cybersécurité doivent être revues et approuvées chaque année par le cadre supérieur ou son (ses) délégué(s) pour vérifier que celles-ci sont toujours nécessaires et valides. Ce processus de révision et d'approbation doit être documenté.
R4	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	E4	Protection de l'information — L'entité responsable doit mettre en œuvre et documenter un programme pour identifier, classer et protéger les informations associées aux actifs électroniques critiques.
R4.1	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.	E4.1	L'information sur les actifs électroniques critiques qui doit être protégée doit inclure, au minimum et peu importe le type de support, les procédures d'exploitation, les listes exigées en vertu de la norme CIP-002, les diagrammes de réseau ou les plans similaires des centres informatiques dans lesquels se trouvent des actifs électroniques critiques, les plans et les schémas des actifs électroniques critiques, les plans et les schémas des centres informatiques dans lesquels se trouvent des actifs électroniques critiques, les plans de rétablissement des opérations, les plans d'intervention en cas d'incident et l'information sur les configurations de sécurité.

Traduction française de la norme de la NERC CIP-003-1

Cyber Security — Security Management Controls

Cybersécurité — Mécanismes de gestion de la sécurité

Ch.	English Version		Version française
R4.2	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	E4.2	L'entité responsable doit classer l'information à protéger en vertu de ce programme en fonction de la sensibilité de l'information sur les actifs électroniques critiques.
R4.3	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	E4.3	L'entité responsable doit, au moins une fois par année, évaluer sa conformité à son programme de protection de l'information sur les actifs électroniques critiques, documenter les résultats de ses analyses et mettre en place un plan d'action pour corriger les lacunes mises au jour par les analyses.
R5	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	E5	Contrôle des accès — L'entité responsable doit documenter et mettre en œuvre un programme pour gérer les privilèges d'accès accordés à l'information protégée sur les actifs électroniques critiques.
R5.1	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	E5.1	L'entité responsable doit maintenir une liste de personnes désignées qui ont la responsabilité d'autoriser les accès électroniques ou physiques à l'information protégée.
R5.1.1	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.	E5.1.1	Les renseignements sur l'identité des membres du personnel doivent comprendre leur nom, leur titre, leur numéro de téléphone au travail ainsi que l'information à laquelle ils ont la responsabilité d'autoriser l'accès.
R5.1.2	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	E5.1.2	La liste des membres du personnel qui autorisent l'accès à l'information protégée doit être vérifiée au moins une fois par année.
R5.2	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	E5.2	L'entité responsable doit revoir au moins une fois par année les privilèges d'accès à l'information protégée pour vérifier qu'ils sont corrects et qu'ils correspondent aux besoins de l'entité responsable ainsi qu'aux responsabilités et aux rôles pertinents de son personnel.
R5.3	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	E5.3	L'entité responsable doit évaluer et documenter, au moins une fois par année, ses processus de vérification des privilèges d'accès à l'information protégée.

Ch.	English Version		Version française
R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	E6.	Contrôle des changements et gestion des configurations — L'entité responsable doit établir et documenter une procédure de contrôle des changements et de gestion des configurations pour l'ajout, la modification, le remplacement ou le retrait d'un élément matériel ou logiciel d'un actif électronique critique et mettre en place des activités de soutien à la gestion des configurations afin d'identifier, de contrôler et de documenter tout changement provenant de l'interne ou du fournisseur qui est apporté aux composants logiciels ou matériels des actifs électroniques critiques dans le cadre du processus de contrôle des changements.

C. Measures / Mesures

	The following measures will be used to demonstrate compliance with the requirements of Standard CIP-003:		Les mesures suivantes serviront à établir la preuve de la conformité aux exigences de la norme CIP-003 :
M1	Documentation of the Responsible Entity's cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.	M1	La documentation sur la politique de sécurité conformément à l'exigence E1. De plus, l'entité responsable doit faire la preuve que sa politique de cybersécurité est disponible conformément à l'exigence E1.2.
M2	Documentation of the assignment of, and changes to, the Responsible Entity's leadership as specified in Requirement R2.	M2	La documentation sur la désignation du cadre supérieur de l'entité responsable, et tout changement concernant cette désignation, conformément à l'exigence E2.
M3	Documentation of the Responsible Entity's exceptions, as specified in Requirement R3.	M3	La documentation de l'entité responsable concernant les exceptions à la politique de cybersécurité, telle que requise par l'exigence E3.
M4	Documentation of the Responsible Entity's information protection program as specified in Requirement R4.	M4	La documentation sur le programme de protection de l'information de l'entité responsable conformément à l'exigence E4.
M5	The access control documentation as specified in Requirement R5.	M5	La documentation sur le contrôle des accès conformément à l'exigence E5.
M6	The Responsible Entity's change control and configuration management documentation as specified in Requirement R6.	M6	La documentation sur le contrôle du changement et la gestion des configurations de l'entité responsable conformément à l'exigence E6.

D. Compliance / Conformité

1.	Compliance Monitoring Process	1.	Processus de surveillance de la conformité
1.1	Compliance Monitoring Responsibility	1.1	Responsabilité pour la surveillance de la conformité

Traduction française de la norme de la NERC CIP-003-1

Cyber Security — Security Management Controls

Cybersécurité — Mécanismes de gestion de la sécurité

Ch.	English Version		Version française
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	Compliance Monitoring Period and Reset Time Frame Annually.	1.2	Période de vérification de la conformité et délai de retour en conformité Annuelle
1.3	Data Retention	1.3	Conservation des données
1.3.1	The Responsible Entity shall keep other documents and records required by Standard CIP-003 from the previous full calendar year.	1.3.1	L'entité responsable doit conserver tout autre document requis en vertu de la norme CIP-003 pour la dernière année civile.
1.3.2	The compliance monitor shall keep audit records for three years.	1.3.2	Le vérificateur de la conformité doit garder les dossiers des audits des trois dernières années civiles.
1.4	Additional Compliance Information	1.4	Autre information sur la conformité
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.
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 (ses) délégué(s). Se reporter à la norme CIP-003, exigence E3. Les exceptions dûment autorisées ne conduiront pas à une non-conformité.
2.	Levels of Non-Compliance	2.	Niveaux de non-conformité
2.1	Level 1:	2.1	Niveau 1 :
2.1.1	Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,	2.1.1	Les changements concernant la désignation du cadre supérieur n'ont pas été documentés en vertu de l'exigence E2.2; ou,
2.1.2	Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,	2.1.2	Les exceptions à la politique de sécurité n'ont pas été documentées dans les 30 jours suivant l'approbation de l'exception; ou,

Ch.	English Version		Version française
2.1.3	An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.	2.1.3	Un programme de protection de l'information pour identifier et classer l'information et les processus de protection de l'information associée aux actifs électroniques critiques n'a pas été vérifié depuis un an.
2.2	Level 2:	2.2	Niveau 2 :
2.2.1	A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,	2.2.1	Une politique de cybersécurité existe, mais elle n'a pas été revue depuis un an; ou,
2.2.2	Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,	2.2.2	Les exceptions à la politique de cybersécurité ne sont pas documentées ou autorisées par le cadre supérieur ou son (ses) délégué(s); ou,
2.2.3	Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,	2.2.3	Les privilèges d'accès à l'information sur les actifs électroniques critiques n'ont pas été revus depuis un an.
2.2.4	The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.	2.2.4	La liste des personnes désignées qui ont la responsabilité d'autoriser l'accès à l'information sur les actifs électroniques critiques n'a pas été revue depuis un an.
2.3	Level 3:	2.3	Niveau 3 :
2.3.1	A senior manager has not been identified in accordance with Requirement R2.1; or,	2.3.1	Les renseignements concernant l'identité d'un cadre supérieur n'ont pas été fournis conformément à l'exigence E2.1; ou,
2.3.2	The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,	2.3.2	La liste des personnes désignées qui ont la responsabilité d'autoriser l'accès électronique ou physique à l'information protégée sur les actifs électroniques critiques n'existe pas; ou,
2.3.3	No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.	2.3.3	Aucun changement aux éléments matériels ou logiciels des actifs électroniques critiques n'a été documenté conformément à l'exigence E6.
2.4	Level 4:	2.4	Niveau 4 :
2.4.1	No cyber security policy exists; or,	2.4.1	Il n'existe pas de politique de cybersécurité; ou,
2.4.2	No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,	2.4.2	Il n'existe pas de programme d'identification et de classement pour la protection de l'information sur les actifs électroniques critiques; ou,

Traduction française de la norme de la NERC CIP-003-1

Cyber Security — Security Management Controls

Cybersécurité — Mécanismes de gestion de la sécurité

Ch.	English Version		Version française
2.4.3	No documented change control and configuration management process exists.	2.4.3	Il n'existe pas de documentation sur le contrôle des changements et il n'y a pas de processus de gestion des configurations.

E. Regional Differences / Différences régionales

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

Version History

Version	Date	Action	Change Tracking
1	06/01/06	Effective Date	New

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	1 ^{er} juin 2006	Date d'entrée en vigueur	Nouvelle norme