

TABLE OF CONTENTS

TABLE DES MATIÈRES

A. INTRODUCTION

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

B. REQUIREMENTS

R1 to R8

C. MEASURES

M1 to M8

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 E8

C. MESURES

M1 à M8

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-007-1

Cyber Security — Systems Security Management

Cybersécurité — Gestion de la sécurité des systèmes

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

A. Introduction / Introduction

1.	Title: Cyber Security — Systems Security Management	1.	Titre : Cybersécurité — Gestion de la sécurité des systèmes
2.	Number: CIP-007-1	2.	Numéro : CIP-007-1
3.	Purpose: Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).	3.	Objet : La norme CIP-007 exige de l'entité responsable qu'elle définisse des méthodes, des processus, et des procédures pour sécuriser les systèmes désignés comme actifs électroniques critiques, ainsi que les actifs électroniques non critiques dans les périmètres de sécurité électroniques.
	Standard CIP-007 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-007 fait partie d'un 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.
4.	Applicability:	4.	Applicabilité :
4.1	Within the text of Standard CIP-007, "Responsible Entity" shall mean :	4.1	Dans le contexte de la norme CIP-007, 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-007-1

Cyber Security — Systems Security Management

Cybersécurité — Gestion de la sécurité des systèmes

Ch.	English Version		Version française
4.2	The following are exempt from Standard CIP-007:	4.2	Les entités suivantes sont exemptées de la norme CIP-007 :
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 liens de communication entre les périmètres de sécurité électroniques.
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 prouvé qu'elles ne détiennent aucun actif informatique critique.
5.	Effective Date: June 1, 2006.	5.	Date d'entrée en vigueur : 1 ^{er} juin 2006

B. Requirements / Exigences

R1	Test procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	E1	Procédures de vérification — L'entité responsable doit s'assurer que les nouveaux actifs électroniques ou que des changements importants aux actifs électroniques en place à l'intérieur du périmètre de sécurité électronique n'ont pas d'impact négatif sur les systèmes de cybersécurité en place. En vertu de la norme CIP-007, un changement important doit minimalement inclure la mise en œuvre de rustines de sécurité, des ensembles de correctifs cumulatifs, des versions des fournisseurs et des mises à jour des systèmes d'exploitation, des applications, des plateformes de base de données ou de tout autre logiciel ou micrologiciel tiers.
R1.1	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	E1.1	L'entité responsable doit créer, mettre en œuvre et gérer des procédures de vérification de la cybersécurité de façon à minimiser les impacts négatifs sur les systèmes de production ou leur exploitation.
R1.2	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	E1.2	L'entité responsable doit montrer dans sa documentation que les vérifications sont exécutées de façon à tenir compte de l'environnement de production.
R1.3	The Responsible Entity shall document test results.	E1.3	L'entité responsable doit documenter le résultat des tests.
R2	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	E2	Ports et services — L'entité responsable doit établir et documenter un processus pour s'assurer que seuls les ports et les services requis pour les activités normales et les activités d'urgence sont activés.

Traduction française de la norme de la NERC CIP-007-1

Cyber Security — Systems Security Management

Cybersécurité — Gestion de la sécurité des systèmes

Ch.	English Version		Version française
R2.1	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	E2.1	L'entité responsable doit activer seulement les ports et les services requis pour les activités normales et les activités d'urgence.
R2.2	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	E2.2	L'entité responsable doit désactiver les autres ports et services, incluant ceux qui servent aux essais, avant la mise en production pour tous les actifs électroniques à l'intérieur des périmètres de sécurité électroniques.
R2.3	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	E2.3	Dans le cas où, à cause de limitations techniques, les ports et services inutilisés ne peuvent pas être désactivés, l'entité responsable doit documenter les mesures compensatoires mises en place pour atténuer l'exposition au risque ou documenter l'acceptation du risque.
R3	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	E3	Gestion des rustines de sécurité — L'entité responsable, de façon séparée ou à l'intérieur du processus de la documentation relative à la gestion des configurations décrite à l'exigence E6 de la norme CIP-003, doit établir et documenter un programme de gestion des rustines de sécurité pour faire la vigie, évaluer, tester, et installer les rustines de cybersécurité applicables pour tous les actifs électroniques à l'intérieur des périmètres de sécurité électroniques.
R3.1	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	E3.1	L'entité responsable doit documenter l'évaluation des rustines de sécurité et des mises à jour de sécurité pour déterminer si elles doivent être déployées dans les 30 jours suivant leur disponibilité.
R3.2	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk	E3.2	L'entité responsable doit documenter la mise en œuvre des rustines de sécurité. Dans tous les cas où la rustine n'est pas installée, l'entité responsable doit documenter les mesures compensatoires mises en place pour atténuer l'exposition au risque ou documenter l'acceptation du risque.
R4	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	E4	Prévention des logiciels malveillants — Là où la technologie le permet, l'entité responsable doit utiliser un logiciel antivirus et d'autres outils de prévention des logiciels malveillants (« maliciels ») pour détecter, prévenir, empêcher, et atténuer l'introduction, l'exposition, et la propagation des logiciels malveillants sur les actifs électroniques à l'intérieur des périmètres de sécurité électroniques.

Traduction française de la norme de la NERC CIP-007-1

Cyber Security — Systems Security Management

Cybersécurité — Gestion de la sécurité des systèmes

Ch.	English Version		Version française
R4.1	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	E4.1	L'entité responsable doit documenter et mettre en œuvre un logiciel antivirus et des outils de prévention des logiciels malveillants. Dans le cas où un logiciel antivirus et un outil de prévention des logiciels malveillants ne sont pas installés, l'entité responsable doit documenter les mesures compensatoires visant à atténuer l'exposition au risque ou documenter l'acceptation du risque.
R4.2	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.	E4.2	L'entité responsable doit documenter et mettre en œuvre un processus pour la mise à jour des « signatures » des logiciels antivirus et des outils de prévention des logiciels malveillants. Le processus doit porter également sur les essais et l'installation des signatures.
R5	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	E5	La gestion des comptes — L'entité responsable doit établir, mettre en œuvre et documenter les contrôles, d'un point de vue technique ainsi que les procédures qui assurent l'authentification et la responsabilité des accès à toutes les activités des usagers, et qui minimisent les risques d'un accès non autorisé à un système.
R5.1	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.	E5.1	L'entité responsable doit s'assurer que les comptes individuels et communs et les autorisations d'accès respectent le principe du « besoin de connaître » selon les fonctions et les tâches de chacun.
R5.1.1	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.	E5.1.1	L'entité responsable doit s'assurer que les comptes utilisateurs sont mis en œuvre tel qu'approuvé par le personnel désigné. Se reporter à l'exigence E5 de la norme CIP-003.
R5.1.2	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	E5.1.2	L'entité responsable doit établir des méthodes, des processus et procédures qui génèrent des journaux contenant suffisamment de détails pour créer des historiques d'utilisation sur les transactions d'accès d'un compte utilisateur pour un minimum de 90 jours.
R5.1.3	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.	E5.1.3	L'entité responsable doit revoir, au minimum une fois par année, les comptes utilisateurs pour s'assurer que les privilèges d'accès sont conformes à l'exigence E5 de la norme CIP-003 et à l'exigence E4 de la norme CIP-004.
R5.2	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	E5.2	L'entité responsable doit mettre en œuvre une politique en vue de minimiser et de gérer la portée et les cas acceptables d'utilisation des comptes administrateurs, communs et des autres comptes génériques avec privilèges en incluant les comptes par défaut.

Traduction française de la norme de la NERC CIP-007-1

Cyber Security — Systems Security Management

Cybersécurité — Gestion de la sécurité des systèmes

Ch.	English Version		Version française
R5.2.1	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	E5.2.1	La politique doit inclure le retrait, la désactivation, ou le changement de nom de ces comptes, lorsque cela est possible. Pour de tels comptes qui doivent rester activés, les mots de passe doivent être modifiés avant de les mettre en service.
R5.2.2	The Responsible Entity shall identify those individuals with access to shared accounts.	E5.2.2	L'entité responsable doit identifier les personnes ayant des accès à des comptes communs.
R5.2.3	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	E5.2.3	Lorsque de tels comptes sont partagés, l'entité responsable doit avoir une politique de gestion d'utilisation de ces comptes en limitant l'accès uniquement aux personnes autorisées, un historique d'utilisation de ces comptes (automatisé ou manuel), et les mesures pour sécuriser les comptes en cas de changement de personnel (promotion ou cessation d'emploi par exemple).
R5.3	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	E5.3	Au minimum, l'entité responsable doit exiger et utiliser des mots de passe, dans le respect des conditions ci-suivantes, si la technologie le permet :
R5.3.1	Each password shall be a minimum of six characters.	E5.3.1	Chaque mot de passe doit avoir un minimum de 6 caractères.
R5.3.2	Each password shall consist of a combination of alpha, numeric, and "special" characters.	E5.3.2	Chaque mot de passe doit être constitué d'une combinaison de lettres, de chiffres, et de caractères spéciaux (non alphanumériques).
R5.3.3	Each password shall be changed at least annually, or more frequently based on risk.	E5.3.3	Chaque mot de passe doit être changé au moins une fois l'an, ou plus fréquemment selon le risque.
R6	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	E6	Surveillance du statut de la sécurité — L'entité responsable doit s'assurer que, pour tous les actifs électroniques à l'intérieur d'un périmètre électronique de sécurité, des outils automatisés ou des processus de contrôle organisationnels soient utilisés, selon les moyens techniques disponibles, pour surveiller les événements systèmes qui relèvent de la cybersécurité.
R6.1	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	E6.1	L'entité responsable doit mettre en œuvre et documenter les procédures et les mécanismes techniques ou procéduraux pour la vérification des événements de sécurité de tous les actifs électroniques à l'intérieur d'un périmètre de sécurité électronique.
R6.2	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	E6.2	Les mécanismes de contrôle de la vérification de la sécurité doivent déclencher des alertes automatiques ou manuelles en cas de cyberincidents de sécurité.

Traduction française de la norme de la NERC CIP-007-1

Cyber Security — Systems Security Management

Cybersécurité — Gestion de la sécurité des systèmes

Ch.	English Version		Version française
R6.3	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP 008.	E6.3	L'entité responsable doit gérer les journaux des événements systèmes relevant de la cybersécurité, là où la technologie le permet, pour soutenir les processus d'intervention tel qu'exigé dans la norme CIP-008.
R6.4	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	E6.4	L'entité responsable doit conserver tous les journaux précisés dans l'exigence E6 durant 90 jours civils.
R6.5	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	E6.5	L'entité responsable doit vérifier les journaux des événements systèmes relevant de la cybersécurité et conserver les preuves de ces vérifications.
R7	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	E7	Destruction et redéploiement — L'entité responsable doit établir des méthodes formelles, des processus, et des procédures pour la disposition ou le redéploiement des actifs électroniques à l'intérieur des périmètres de sécurité électroniques tels que définis et documentés dans la norme CIP-005.
R7.1	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	E7.1	Avant le retrait de tels actifs, l'entité responsable doit détruire ou effacer le médium de sauvegarde des données afin de prévenir l'extraction non autorisée de données sensibles de cybersécurité ou de données de fiabilité.
R7.2	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	E7.2	Avant le redéploiement de tels actifs, l'entité responsable doit, au minimum, effacer les données de tous les médias de sauvegarde pour prévenir l'extraction non autorisée de données sensibles de cybersécurité ou de données de fiabilité.
R7.3	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	E7.3	L'entité responsable doit conserver des preuves que ces actifs ont été retirés ou redéployés selon les procédures documentées.
R8	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	E8	Analyse de la cybervulnérabilité — L'entité responsable doit faire une analyse de la cybervulnérabilité de tous les actifs électroniques à l'intérieur du périmètre de sécurité électronique au moins une fois par année. L'analyse de la vulnérabilité doit inclure, au minimum, un des points suivants :
R8.1	A document identifying the vulnerability assessment process;	E8.1	La documentation décrivant la procédure d'analyse de la vulnérabilité.
R8.2	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	E8.2	Une vérification faisant état que seuls les ports et les services nécessaires pour l'exploitation des actifs électroniques à l'intérieur du périmètre de sécurité électronique sont actifs.

Traduction française de la norme de la NERC CIP-007-1

Cyber Security — Systems Security Management

Cybersécurité — Gestion de la sécurité des systèmes

Ch.	English Version		Version française
R8.3	A review of controls for default accounts; and,	E8.3	Une vérification des mécanismes de contrôle pour les comptes par défaut, et,
R8.4	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	E8.4	La documentation des résultats de l'analyse, du plan d'action pour corriger ou atténuer les vulnérabilités découvertes au cours de l'analyse et de l'état d'avancement du plan d'action.
R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	E9	Révision et mise à jour de la documentation — L'entité responsable doit réviser et mettre à jour la documentation décrite dans la norme CIP-007 au moins une fois par année. Les changements suivant une modification des systèmes ou des contrôles doivent être documentés dans les 90 jours civils suivant le changement.

C. Measures / Mesures

	The following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:		Les mesures suivantes serviront à établir la preuve de la conformité aux exigences de la norme CIP-007 :
M1	Documentation of the Responsible Entity's security test procedures as specified in Requirement R1.	M1	La documentation sur les procédures d'essais de sécurité de l'entité responsable conformément à l'exigence E1.
M2	Documentation as specified in Requirement R2.	M2	La documentation conformément à l'exigence E2.
M3	Documentation and records of the Responsible Entity's security patch management program, as specified in Requirement R3.	M3	La documentation et les dossiers relatifs au programme de gestion des rustines de sécurité de l'entité responsable conformément à l'exigence E3.
M4	Documentation and records of the Responsible Entity's malicious software prevention program as specified in Requirement R4.	M4	La documentation et les dossiers de l'entité responsable concernant le programme de protection contre les logiciels malveillants conformément à l'exigence E4.
M5	Documentation and records of the Responsible Entity's account management program as specified in Requirement R5.	M5	La documentation et les dossiers de l'entité responsable sur le programme de gestion des comptes conformément à l'exigence E5.
M6	Documentation and records of the Responsible Entity's security status monitoring program as specified in Requirement R6.	M6	La documentation et les dossiers de l'entité responsable sur son programme de gestion de l'état de la sécurité conformément à l'exigence E6.
M7	Documentation and records of the Responsible Entity's program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.	M7	La documentation et les dossiers de l'entité responsable sur le programme de retrait ou de redéploiement des actifs électroniques conformément à l'exigence E7.

Ch.	English Version		Version française
M8	Documentation and records of the Responsible Entity’s annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.	M8	La documentation et les dossiers de l'entité responsable sur l'analyse de vulnérabilité de tous les actifs électroniques à l'intérieur des périmètres de sécurité électroniques conformément à l'exigence E8.
M9	Documentation and records demonstrating the review and update as specified in Requirement R9.	M9	La documentation et les dossiers qui démontrent les révisions et la mise en jour conformément à l'exigence E9.

D. Compliance / Conformité

1.	Compliance Monitoring Process	1.	Processus de vérification de la conformité
1.1	Compliance Monitoring Responsibility	1.1	Responsabilité de la vérification de la conformité
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 all documentation and records from the previous full calendar year.	1.3.1	L'entité responsable doit conserver l'ensemble de la documentation et des dossiers de la dernière année civile.
1.3.2	The Responsible Entity shall retain security-related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008 Requirement R2.	1.3.2	L'entité responsable doit conserver les journaux des événements systèmes relevant de la sécurité pendant 90 jours civils, à moins que la période de rétention soit plus longue, en vertu de l'exigence E2 de la norme CIP-008.
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	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	Les entités responsables doivent faire la preuve de leur conformité au moyen d'une autocertification ou d'une vérification, selon ce que déterminera le vérificateur de la conformité.

Traduction française de la norme de la NERC CIP-007-1

Cyber Security — Systems Security Management

Cybersécurité — Gestion de la sécurité des systèmes

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 ne peut se conformer 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.	Levels of Non-Compliance	2.	Niveaux de non-conformité
2.1	Level 1:	2.1	Niveau 1 :
2.1.1	System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or	2.1.1	Les systèmes de contrôle de la sécurité sont en place, mais il n'y a pas de documentation sur l'une des mesures (M1 à M9) de la norme CIP-007; ou,
2.1.2	One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,	2.1.2	Un des documents exigés par la norme CIP-007 n'a pas été révisé depuis un an en vertu de l'exigence E9; ou,
2.1.3	One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,	2.1.3	Un des systèmes de contrôle de la sécurité documenté n'a pas été mis à jour dans les 90 jours suivant le changement conformément à l'exigence E9; ou,
2.1.4	Any one of:	2.1.4	Une occurrence des violations suivantes :
	<ul style="list-style-type: none"> • Authorization rights and access privileges have not been reviewed during the previous full calendar year; or, 		<ul style="list-style-type: none"> • Les droits d'autorisation et les privilèges d'accès n'ont pas été révisés depuis la dernière année civile; ou,
	<ul style="list-style-type: none"> • A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or, 		<ul style="list-style-type: none"> • Une différence existe dans n'importe quel des registres des événements système relevant de la cybersécurité de plus de sept jours; ou,
	<ul style="list-style-type: none"> • Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability. 		<ul style="list-style-type: none"> • Les rustines de sécurité n'ont pas été analysées pour savoir si elles doivent être déployées dans les 30 jours suivant leur disponibilité; ou,
2.2	Level 2:	2.2	Niveau 2 :
2.2.1	System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,	2.2.1	Les systèmes de contrôle de la sécurité sont en place, mais il n'y a pas de documentation sur deux des mesures (M1 à M9) de la norme CIP-007; ou,
2.2.2	Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.	2.2.2	Deux occurrences de n'importe quelle combinaison des violations énumérées dans la non-conformité niveau 1, 2.1.4 au cours de la même période de conformité.
2.3	Level 3:	2.3	Niveau 3 :

Traduction française de la norme de la NERC CIP-007-1

Cyber Security — Systems Security Management

Cybersécurité — Gestion de la sécurité des systèmes

Ch.	English Version		Version française
2.3.1	System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,	2.3.1	Les systèmes de contrôle de la sécurité sont en place, mais il n'y a pas de documentation sur trois des mesures (M1 à M9) de la norme CIP-007; ou,
2.3.2	Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.	2.3.2	Trois occurrences de n'importe quelle combinaison des violations énumérées dans la non-conformité niveau 1, 2.1.4 au cours de la même période de conformité.
2.4	Level 4:	2.4	Niveau 4 :
2.4.1	System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,	2.4.1	Les systèmes de contrôle de la sécurité sont en place, mais il n'y a pas de documentation sur quatre ou plus des mesures (M1 à M9) de la norme CIP-007; ou,
2.4.2	Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.	2.4.2	Quatre occurrences de n'importe quelle combinaison des violations énumérées dans la non-conformité niveau 1, 2.1.4 dans la même période de conformité.
2.4.3	No logs exist.	2.4.3	Aucun journal d'exploitation n'existe.

E. Regional Differences / Différences régionales

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

Traduction française de la norme de la NERC CIP-007-1

Cyber Security — Systems Security Management Cybersécurité — Gestion de la sécurité des systèmes

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