

Traduction française de la norme de la NERC CIP-009-1

Cyber Security — Recovery Plans for Critical Cyber Assets

Cybersécurité — Plan de rétablissement pour les actifs électroniques critiques

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 pour 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-009-1

Cyber Security — Recovery Plans for Critical Cyber Assets

Cybersécurité — Plan de rétablissement pour les actifs électroniques critiques

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

A. Introduction / Introduction

1.	Title: Cyber Security — Recovery Plans for Critical Cyber Assets	1.	Titre : Cybersécurité — Plan de rétablissement pour les actifs électroniques critiques
2.	Number: CIP-009-1	2.	Numéro : CIP-009-1
3.	Purpose: Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.	3.	Objet : La norme CIP-009 exige que le ou les plans de rétablissement soient en place pour les actifs électroniques critiques et que ces plans reposent sur les techniques et les pratiques en matière de continuité des affaires et de rétablissement après désastre.
	Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.		La norme CIP-009 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 qui s'imposent.
4.	Applicability:	4.	Applicabilité :
4.1	Within the text of Standard CIP-009, “Responsible Entity” shall mean :	4.1	Dans le contexte de la norme CIP-009, 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-009-1

Cyber Security — Recovery Plans for Critical Cyber Assets

Cybersécurité — Plan de rétablissement pour les actifs électroniques critiques

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 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 électronique critique.
5.	Effective Date: June 1, 2006.	5.	Date d'entrée en vigueur : 1 ^{er} juin 2006

B. Requirements / Exigences

R1	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	E1	Plans de rétablissement — L'entité responsable doit créer et revoir annuellement des plans de rétablissement des actifs électroniques critiques. Les plans de rétablissement doivent traiter au minimum des points suivants :
R1.1	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	E1.1	Préciser les interventions prévues à l'égard d'événements ou de conditions de durée et de sévérité variables qui déclencheraient la mise en œuvre du ou des plans de rétablissement.
R1.2	Define the roles and responsibilities of responders.	E1.2	Définir les rôles et les responsabilités des intervenants.
R2	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	E2	Exercices — Les plans de rétablissement doivent être testés au moins une fois par année. Les tests des plans de rétablissement varient entre un simple exercice sur papier et un exercice opérationnel complet, ou un cas réel.
R3	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	E3	Contrôle des changements — Les plans de rétablissement doivent être mis à jour pour refléter tout changement ou les leçons apprises par suite d'un exercice ou d'un rétablissement après un incident réel. Les mises à jour doivent être transmises au personnel responsable de l'activation et de la mise en œuvre des plans de rétablissement dans les 90 jours civils suivant les changements.

Traduction française de la norme de la NERC CIP-009-1

Cyber Security — Recovery Plans for Critical Cyber Assets

Cybersécurité — Plan de rétablissement pour les actifs électroniques critiques

Ch.	English Version		Version française
R4	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	E4	Matériel de secours et rétablissement — Les plans de rétablissement doivent inclure les processus et les procédures pour la sauvegarde et le stockage des informations utiles au rétablissement des actifs électroniques critiques. Par exemple, le matériel de secours peut inclure des pièces ou des composantes électroniques en réserve, de la documentation papier sur les paramètres de configuration, les sauvegardes sur bande, etc.
R5	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	E5	Tests des médias de sauvegarde — Les données essentielles au rétablissement qui sont enregistrées sur des médias en copie de secours doivent être testées au moins une fois par année pour s'assurer qu'elles sont disponibles. Les tests peuvent être effectués hors site.

C. Measures / Mesures

	The following measures will be used to demonstrate compliance with the requirements of Standard CIP-009:		Les mesures suivantes serviront à établir la preuve de la conformité aux exigences de la norme CIP-009 :
M1	Recovery plan(s) as specified in Requirement R1.	M1	Les plans de rétablissement conformément à l'exigence E1.
M2	Records documenting required exercises as specified in Requirement R2.	M2	Les dossiers documentant les exercices requis conformément à l'exigence E2.
M3	Documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.	M3	La documentation des changements apportés aux plans de rétablissement et la documentation de toutes les communications conformément à l'exigence E3.
M4	Documentation regarding backup and storage of information as specified in Requirement R4.	M4	La documentation de la sauvegarde et du stockage des données conformément à l'exigence E4.
M5	Documentation of testing of backup media as specified in Requirement R5.	M5	La documentation des tests sur les médias de sauvegarde conformément à l'exigence E5.

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.

Traduction française de la norme de la NERC CIP-009-1

Cyber Security — Recovery Plans for Critical Cyber Assets

Cybersécurité — Plan de rétablissement pour les actifs électroniques critiques

Ch.	English Version		Version française
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 documentation required by Standard CIP-009 from the previous full calendar year.	1.3.1	L'entité responsable doit conserver toute la documentation de la dernière année civile complète conformément à la norme CIP-009.
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	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.
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 pour lesquels l'entité responsable n'est pas conforme à sa politique de cybersécurité doivent être documentés en tant qu'exceptions 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	Recovery plan(s) exist and are exercised, but do not contain all elements as specified in Requirement R1; or,	2.1.1	Le ou les plans de rétablissement existent et sont testés, mais ils ne contiennent pas tous les éléments requis en vertu de l'exigence E1; ou,
2.1.2	Recovery plan(s) are not updated and personnel are not notified within ninety calendar days of the change.	2.1.2	Le ou les plans de rétablissement ne sont pas mis à jour et le personnel n'est pas averti dans les 90 jours civils qui suivent un changement.
2.2	Level 2:	2.2	Niveau 2 :
2.2.1	Recovery plan(s) exist, but have not been reviewed during the previous full calendar year; or,	2.2.1	Le ou les plans de rétablissement existent, mais ils n'ont pas été revus au cours de la dernière année civile complète; ou,

Traduction française de la norme de la NERC CIP-009-1

Cyber Security — Recovery Plans for Critical Cyber Assets

Cybersécurité — Plan de rétablissement pour les actifs électroniques critiques

Ch.	English Version		Version française
2.2.2	Documented processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets do not exist.	2.2.2	Les processus et les procédures documentés de la sauvegarde et du stockage des données utiles au rétablissement des actifs électroniques critiques n'existent pas.
2.3	Level 3:	2.3	Niveau 3 :
2.3.1	Testing of information stored on backup media to ensure that the information is available has not been performed at least annually; or,	2.3.1	Les tests des médias de sauvegarde permettant de vérifier que les données sont disponibles n'ont pas été faits au moins une fois par année; ou,
2.3.2	Recovery plan(s) exist, but have not been exercised during the previous full calendar year.	2.3.2	Les plans de rétablissement existent, mais ils n'ont pas fait l'objet d'exercices au cours de la dernière année civile.
2.4	Level 4:	2.4	Niveau 4 :
2.4.1	No recovery plan(s) exist; or,	2.4.1	Il n'y a pas de plan de rétablissement; ou,
2.4.2	Backup of information required to successfully restore Critical Cyber Assets does not exist.	2.4.2	La copie de sauvegarde des données nécessaires au rétablissement des actifs électroniques critiques n'existe pas.

E. Regional Differences / Différences régionales

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

Version History

Version	Date	Action	Change Tracking
0	06/01/06	Effective Date	New

Historique des versions

Version	Date	Intervention	Suivi des modifications
0	1 ^{er} juin 2006	Date d'entrée en vigueur	Nouvelle norme