

TABLE OF CONTENTS

TABLE DES MATIÈRES

A. INTRODUCTION

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

B. REQUIREMENTS

R1 and R2

C. MEASURES

M1 and M2

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 et E2

C. MESURES

M1 et M2

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-008-1

Cyber Security — Incident Reporting and Response Planning

Cybersécurité — Déclaration des incidents et planification des mesures d'urgence

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

A. Introduction / Introduction

1.	Title: Cyber Security — Incident Reporting and Response Planning	1.	Titre : Cybersécurité — Déclaration des incidents et planification des mesures d'urgence
2.	Number: CIP-008-1	2.	Numéro : CIP-008-1
3.	Purpose: Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.	3.	Objet : La norme CIP-008 exige l'identification, la classification, l'intervention, et la déclaration des cyberincidents liés aux actifs électroniques critiques.
	Standard CIP-008 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-008 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-008, "Responsible Entity" shall mean :	4.1	Dans le contexte de la norme CIP-008, 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-008-1

Cyber Security — Incident Reporting and Response Planning

Cybersécurité — Déclaration des incidents et planification des mesures d'urgence

Ch.	English Version		Version française
4.2	The following are exempt from Standard CIP-008 :	4.2	Les entités suivantes sont exemptées de la norme CIP-008 :
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 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 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	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	E1	Plan d'intervention en cas de cyberincidents de sécurité — L'entité responsable doit développer et gérer un plan des mesures d'urgence en cas de cyberincidents de sécurité. Le plan des mesures d'urgence en cas de cyberincidents de sécurité doit inclure au moins les points suivants :
R1.1	Procedures to characterize and classify events as reportable Cyber Security Incidents.	E1.1	Les procédures permettant de caractériser et de classer les événements à déclarer en tant que cyberincidents de sécurité.
R1.2	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.	E1.2	Les interventions, incluant les rôles et les responsabilités de l'équipe d'intervention en cas d'incidents, les procédures de gestion des incidents et les plans de communication.
R1.3	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.	E1.3	Le processus pour la déclaration des cyberincidents de sécurité au <i>Electricity Sector Information Sharing and Analysis Center (ES ISAC)</i> . L'entité responsable doit s'assurer que tous les cyberincidents de sécurité à déclarer sont déclarés au <i>ES ISAC</i> directement ou par un intermédiaire.
R1.4	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.	E1.4	Le processus pour la mise à jour du plan d'intervention en cas de cyberincidents de sécurité dans les 90 jours civils suivant tout changement.
R1.5	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	E1.5	Le processus pour s'assurer que le plan d'intervention en cas de cyberincidents de sécurité est revu au moins une fois par année.

Traduction française de la norme de la NERC CIP-008-1

Cyber Security — Incident Reporting and Response Planning

Cybersécurité — Déclaration des incidents et planification des mesures d'urgence

Ch.	English Version		Version française
R1.6	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	E1.6	Le processus pour s'assurer que le plan d'intervention en cas de cyberincidents de sécurité est testé au moins une fois par année. Les tests du plan des mesures d'urgence en cas d'incidents peuvent varier d'un simple exercice sur papier à un exercice opérationnel complet, ou même à un cas réel.
R2	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	E2	Documentation sur les cyberincidents de sécurité — L'entité responsable doit conserver la documentation pertinente relative à un cyberincident de sécurité déclaré en vertu de l'exigence E1.1 pour une période de trois années civiles.

C. Measures / Mesures

	The following measures will be used to demonstrate compliance with the requirements of Standard CIP-008:		Les mesures suivantes serviront à établir la preuve de la conformité aux exigences de la norme CIP-008 :
M1	The Cyber Security Incident response plan as indicated in R1 and documentation of the review, updating, and testing of the plan	M1	Le plan de rétablissement en cas de cyberincidents de sécurité en vertu de l'exigence E1 et la documentation sur les revues, la mise à jour, et les tests du plan.
M2	All documentation as specified in Requirement R2.	M2	Toute la documentation requise en vertu de l'exigence E2.

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

Traduction française de la norme de la NERC CIP-008-1

Cyber Security — Incident Reporting and Response Planning

Cybersécurité — Déclaration des incidents et planification des mesures d'urgence

Ch.	English Version		Version française
1.3.1	The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008 for the previous full calendar year.	1.3.1	L'entité responsable doit conserver toute la documentation pendant une année civile complète, sauf dans le cas des déclarations de cyberincident de sécurité prévues par la norme CIP-008.
1.3.2	The compliance monitor shall keep audit records for three calendar 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 ne peut pas se conformer 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.
1.4.3	The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.	1.4.3	L'entité responsable ne doit pas faire d'exception dans ses politiques de cybersécurité en ce qui a trait à la création d'un plan d'intervention en cas de cyberincidents de sécurité.
1.4.4	The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.	1.4.4	L'entité responsable ne devrait pas faire d'exception dans ses politiques de sécurité en ce qui a trait à la déclaration des cyberincidents de sécurité au <i>ES ISAC</i> .
2.	Levels of Non-Compliance	2.	Niveaux de non-conformité
2.1	Level 1: A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.	2.1	Niveau 1 : Un plan d'intervention en cas de cyberincidents de sécurité existe, mais il n'a pas été mis à jour dans les 90 jours civils suivant un changement.
2.2	Level 2:	2.2	Niveau 2 :
2.2.1	A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,	2.2.1	Un plan des mesures d'urgence en cas de cyberincidents de sécurité existe, mais il n'a pas été revu au cours de la dernière année civile complète; ou,
2.2.2	A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,	2.2.2	Le plan d'intervention en cas de cyberincidents de sécurité n'a pas été testé au cours de la dernière année civile complète; ou,

Traduction française de la norme de la NERC CIP-008-1

Cyber Security — Incident Reporting and Response Planning

Cybersécurité — Déclaration des incidents et planification des mesures d'urgence

Ch.	English Version		Version française
2.2.3	Records related to reportable Cyber Security Incidents were not retained for three calendar years.	2.2.3	Les dossiers des cyberincidents de sécurité à déclarer n'ont pas été pas conservés pour une période de trois années civiles.
2.3	Level 3:	2.3	Niveau 3 :
2.3.1	A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,	2.3.1	Un plan d'intervention en cas de cyberincidents de sécurité existe, mais il ne comprend pas les éléments prévus par les exigences E1.1, E1.2, et E1.3 de la norme CIP-008; ou,
2.3.2	A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.	2.3.2	Un cyberincident de sécurité à déclarer s'est produit, mais il n'a pas été déclaré au <i>ES ISAC</i> .
2.4	Level 4:	2.4	Niveau 4 :
	A Cyber Security Incident response plan does not exist.		Le plan d'intervention en cas de cyberincidents de sécurité n'existe pas.

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