

Telecommunications

Télécommunications

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 and M4

D. COMPLIANCE

- 1. Compliance Monitoring Process
 - 1.1 Compliance Monitoring Responsibility
 - 1.2 Compliance Monitoring and Reset Time Frame
 - 1.3 Data Retention
 - 1.4 Additional Compliance Information
- 2. Levels of Non-Compliance for Transmission Operator, Balancing Authority or Reliability Coordinator:
 - 2.1 Level 1
 - 2.2 Level 2
 - 2.3 Level 3
 - 2.4 Level 4
- 3. Levels of Non-Compliance – NERCnet User Organization:
 - 3.1 Level 1
 - 3.2 Level 2

A. INTRODUCTION

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

B. EXIGENCES

E1 à E6

C. MESURES

M1 et M4

D. CONFORMITÉ

- 1. Processus de vérification de la conformité
 - 1.1 Responsabilité de la vérification de la conformité
 - 1.2 Périodicité de la 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 pour l'exploitant du réseau de transport, le responsable de l'équilibrage ou le coordonnateur de la fiabilité :
 - 2.1 Niveau 1
 - 2.2 Niveau 2
 - 2.3 Niveau 3
 - 2.4 Niveau 4
- 3. Niveaux de non-conformité – Organisation utilisatrice du NERCnet :
 - 3.1 Niveau 1
 - 3.2 Niveau 2

Traduction française de la norme de la NERC COM-001-1

Telecommunications

Télécommunications

3.3 Level 3

3.3 Niveau 3

3.4 Level 4

3.4 Niveau 4

E. REGIONAL DIFFERENCES

E. DIFFÉRENCES RÉGIONALES

VERSION HISTORY

HISTORIQUE DES VERSIONS

ATTACHMENT 1-COM-001 – NERCNET SECURITY POLICY

**ANNEXE 1-COM-001 – POLITIQUE DE SÉCURITÉ
RELATIVE AU NERCNET**

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

A. Introduction / Introduction

1.	Title: Telecommunications	1.	Titre : Télécommunications
2.	Number: COM-001-1	2.	Numéro : COM-001-1
3.	Purpose: Each Reliability Coordinator, Transmission Operator and Balancing Authority needs adequate and reliable telecommunications facilities internally and with others for the exchange of Interconnection and operating information necessary to maintain reliability.	3.	Objet : Chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit disposer d'installations de télécommunications adéquates et fiables entre les membres de son personnel ainsi qu'avec d'autres entités, afin d'assurer l'échange d'information nécessaire au maintien de la fiabilité, qui se rapporte à l'interconnexion et à l'exploitation.
4.	Applicability	4.	Applicabilité :
4.1	Transmission Operators	4.1	Exploitants du réseau de transport
4.2	Balancing Authorities	4.2	Responsables de l'équilibrage
4.3	Reliability Coordinators.	4.3	Coordonnateurs de la fiabilité
4.4	NERCNet User Organizations.	4.4	Organisations utilisatrices du NERCnet
5.	Effective Date : January 1, 2007	5.	Date d'entrée en vigueur : 1 ^{er} janvier 2007

B. Requirements / Exigences

R1	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information:	E1	Chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit fournir des installations de télécommunications adéquates et sûres en vue d'échanger des informations d'interconnexion et d'exploitation :
R1.1	Internally.	E1.1	à l'interne,
R1.2	Between the Reliability Coordinator and its Transmission Operators and Balancing Authorities.	E1.2	entre le coordonnateur de la fiabilité et ses exploitants du réseau de transport et responsables de l'équilibrage,
R1.3	With other Reliability Coordinators, Transmission Operators, and Balancing Authorities as necessary to maintain reliability.	E1.3	avec d'autres coordonnateurs de la fiabilité, exploitants du réseau de transport et responsables de l'équilibrage, lorsque nécessaire pour maintenir la fiabilité.
R1.4	Where applicable, these facilities shall be redundant and diversely routed.	E1.4	Là où c'est pertinent, ces installations doivent être redondante et utiliser une diversité de parcours.

Traduction française de la norme de la NERC COM-001-1

Telecommunications

Télécommunications

Ch.	English Version		Version française
R2	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall manage, alarm, test and/or actively monitor vital telecommunications facilities. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications.	E2	Chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit gérer, doter de mécanismes d'alarme, mettre à l'essai ou surveiller activement les installations de télécommunications vitales. Une attention spéciale doit être accordée aux installations de télécommunications d'urgence et aux équipements qui ne sont pas employés pour les communications courantes.
R3	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide a means to coordinate telecommunications among their respective areas. This coordination shall include the ability to investigate and recommend solutions to telecommunications problems within the area and with other areas.	E3	Chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit se doter de moyens de coordonner les télécommunications entre leurs zones respectives. Cette coordination doit comprendre la capacité d'effectuer des enquêtes et de recommander des solutions aux problèmes de télécommunications à l'intérieur de leur zone et avec d'autres zones.
R4	Unless agreed to otherwise(*), each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use English as the language for all communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected Bulk Electric System. Transmission Operators and Balancing Authorities may use an alternate language for internal operations. (*) It is agreed that communication with entities located in the Province of Québec will be in French.	E4	Sauf s'il a été convenu de procéder autrement (*), chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit employer l'anglais pour toutes les communications au sein du personnel d'exploitation responsable des contrôles de la production en temps réel et de l'exploitation du réseau de transport principal interconnecté. Les exploitants du réseau de transport et les responsables de l'équilibrage peuvent utiliser une autre langue pour leurs activités internes. (*) Il est convenu que les communications avec les entités situées au Québec se font en français.
R5	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall have written operating instructions and procedures to enable continued operation of the system during the loss of telecommunications facilities.	E5	Chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit disposer d'instructions et de procédures d'exploitation écrites, permettant l'exploitation continue du système en cas de défaillance des installations de télécommunications.
R6	Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001, "NERCNet Security Policy."	E6	Chaque organisation utilisatrice du NERCnet doit adhérer aux dispositions de l'annexe 1-COM-001, intitulée « Politique de sécurité relative au NERCnet ».

Telecommunications

Télécommunications

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

C. Measures / Mesures

M1	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have and provide upon request evidence that could include, but is not limited to communication facility test-procedure documents, records of testing, and maintenance records for communication facilities or equivalent that will be used to confirm that it manages, alarms, tests and/or actively monitors vital telecommunications facilities. (Requirement 2 part 1).	M1	Chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit détenir et fournir sur demande des éléments de preuve qui peuvent comprendre, sans s'y limiter, les documents sur la mise à l'essai des installations de communications, les registres d'essai et les dossiers de maintenance des installations de télécommunications, ou l'équivalent, qui serviront à confirmer qu'il gère, dote de mécanismes d'alarmes, teste ou surveille activement les installations de télécommunications vitales. (exigence E2, partie 1).
M2	The Reliability Coordinator, Transmission Operator or Balancing Authority shall have and provide upon request evidence that could include, but is not limited to operator logs, voice recordings or transcripts of voice recordings, electronic communications, or equivalent, that will be used to determine compliance to Requirement 4.	M2	Le coordonnateur de la fiabilité, l'exploitant du réseau de transport ou le responsable de l'équilibrage doit détenir et fournir sur demande les éléments de preuve qui peuvent comprendre, sans s'y limiter, les journaux d'exploitation, les enregistrements vocaux ou la transcription d'enregistrements vocaux, les communications électroniques, ou l'équivalent, qui serviront à déterminer la conformité à l'exigence E4.
M3	Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have and provide upon request its current operating instructions and procedures, either electronic or hard copy that will be used to confirm that it meets Requirement 5.	M3	Chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit détenir et fournir sur demande ses instructions et procédures d'exploitation en vigueur, sous forme électronique ou papier, qui permettront de confirmer qu'il satisfait à l'exigence E5.
M4	The NERCnet User Organization shall have and provide upon request evidence that could include, but is not limited to documented procedures, operator logs, voice recordings or transcripts of voice recordings, electronic communications, etc that will be used to determine if it adhered to the (User Accountability and Compliance) requirements in Attachment 1-COM-001. (Requirement 6).	M4	L'organisation utilisatrice du NERCnet doit détenir et fournir sur demande les éléments de preuve qui peuvent comprendre, sans s'y limiter, les procédures documentées, les journaux d'exploitation, les enregistrements vocaux ou la transcription d'enregistrements vocaux, les communications électroniques, etc., qui serviront à déterminer la conformité aux exigences (en matière de responsabilité et de conformité) énoncées à l'annexe 1-COM-001. (exigence E6).

D. Compliance / Conformité

1.	Compliance Monitoring Process	1.	Processus de vérification de la conformité
----	-------------------------------	----	--

Telecommunications

Télécommunications

Ch.	English Version		Version française
1.1	<p>Compliance Monitoring Responsibility</p> <p>NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations</p> <p>Regional Reliability Organizations shall be responsible for compliance monitoring of all other entities</p>	1.1	<p>Responsabilité de la vérification de la conformité</p> <p>La NERC est responsable de la vérification de la conformité des organisations régionales de fiabilité.</p> <p>Les organisations régionales de fiabilité sont responsables de la vérification de la conformité de toutes les autres entités.</p>
1.2	<p>Compliance Monitoring and Reset Time Frame</p> <p>One or more of the following methods will be used to assess compliance:</p> <ul style="list-style-type: none"> ▪ Self-certification (Conducted annually with submission according to schedule.) ▪ Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.) ▪ Periodic Audit (Conducted once every three years according to schedule.) ▪ Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 calendar days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.) <p>The Performance-Reset Period shall be 12 months from the last finding of non-compliance.</p>	1.2	<p>Périodicité de la vérification de la conformité et délai de retour en conformité</p> <p>Une ou plusieurs des méthodes suivantes serviront à évaluer la conformité :</p> <ul style="list-style-type: none"> ▪ l'autocertification (effectuée chaque année avec présentation d'un rapport selon l'échéancier établi) ; ▪ les audits ponctuels (effectués à tout moment avec préavis pouvant aller jusqu'à 30 jours) ; ▪ l'audit périodique (effectué tous les trois ans, selon l'échéancier établi) ; ▪ les enquêtes sur incident (La notification qu'une enquête sera ouverte doit être faite dans les 60 jours suivant un événement ou une plainte de non-conformité. L'entité a jusqu'à 30 jours civils pour se préparer à l'enquête. Une entité peut demander une prolongation de la période de préparation et cette demande sera évaluée au cas par cas par le vérificateur de la conformité.) <p>Le délai de retour en conformité est de 12 mois à partir de la dernière constatation de non-conformité.</p>

Telecommunications

Télécommunications

Ch.	English Version		Version française
1.3	<p>Data Retention</p> <p>For Measure 1 each Reliability Coordinator, Transmission Operator, Balancing Authority shall keep evidence of compliance for the previous two calendar years plus the current year.</p> <p>For Measure 2 each Reliability Coordinator, Transmission Operator, and Balancing Authority shall keep 90 days of historical data (evidence).</p> <p>For Measure 3, each Reliability Coordinator, Transmission Operator, Balancing Authority shall have its current operating instructions and procedures to confirm that it meets Requirement 5.</p> <p>For Measure 4, each Reliability Coordinator, Transmission Operator, Balancing Authority and NERCnet User Organization shall keep 90 days of historical data (evidence).</p> <p>If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.</p> <p>Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor.</p> <p>The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.</p>	1.3	<p>Conservation des données</p> <p>Pour la mesure 1, chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit conserver les éléments de preuve de sa conformité pour les deux années civiles précédentes en plus de l'année en cours.</p> <p>Pour la mesure 2, chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit conserver un historique (éléments de preuve) de 90 jours de données.</p> <p>Pour la mesure 3, chaque coordonnateur de la fiabilité, exploitant du réseau de transport et responsable de l'équilibrage doit détenir ses instructions et procédures d'exploitation en vigueur afin de confirmer sa conformité à l'exigence E5.</p> <p>Pour la mesure 4, chaque coordonnateur de la fiabilité, exploitant du réseau de transport, responsable de l'équilibrage et organisation utilisatrice du NERCnet doit conserver un historique (éléments de preuve) de 90 jours de données.</p> <p>Si une entité est jugée non conforme, l'entité doit conserver l'information sur la non-conformité jusqu'à ce qu'elle soit jugée conforme, ou pendant deux ans en plus de l'année en cours, selon la plus longue de ces deux périodes.</p> <p>Les preuves utilisées dans le cadre d'une enquête sur incident doivent être conservées par l'entité qui en fait l'objet durant une période d'un an à compter de la date de la fin de l'enquête, telle que fixée par le vérificateur de la conformité.</p> <p>Le vérificateur de la conformité doit conserver le dernier rapport de vérification périodique ainsi que tous les rapports de conformité subséquents demandés et soumis.</p>
1.4	<p>Additional Compliance Information</p> <p>Attachment 1-COM-001 – NERCnet Security Policy</p>	1.4	<p>Autre information sur la conformité</p> <p>Annexe 1-COM-001 – Politique de sécurité relative au NERCnet.</p>
2.	<p>Levels of Non-Compliance for Transmission Operator, Balancing Authority or Reliability Coordinator:</p>	2.	<p>Niveaux de non-conformité pour l'exploitant du réseau de transport, le responsable de l'équilibrage et le coordonnateur de la fiabilité :</p>
2.1	<p>Level 1: Not applicable</p>	2.1	<p>Niveau 1 : Sans objet.</p>
2.2	<p>Level 2: Not applicable</p>	2.2	<p>Niveau 2 : Sans objet.</p>

Traduction française de la norme de la NERC COM-001-1

Telecommunications

Télécommunications

Ch.	English Version		Version française
2.3	Level 3: There shall be a separate Level 3 non-compliance, for every one of the following requirements that is in violation:	2.3	Niveau 3 : Il y a un niveau de non-conformité de niveau 3 distinct pour chacune des situations suivantes :
2.3.1	The Transmission Operator, Balancing Authority or Reliability Coordinator used a language other than English without agreement as specified in R4.	2.3.1	L'exploitant du réseau de transport, le responsable de l'équilibrage ou le coordonnateur de la fiabilité a utilisé une autre langue que l'anglais sans qu'il y ait entente à ce sujet (exigence E4).
2.3.2	There are no written operating instructions and procedures to enable continued operation of the system during the loss of telecommunication facilities as specified in R5.	2.3.2	Il n'y a pas d'instructions ou de procédures d'exploitation écrites visant à permettre l'exploitation continue du réseau en cas de panne des installations de télécommunications, contrairement à ce que prévoit l'exigence E5.
2.4	Level 4: Telecommunication systems are not actively monitored, tested, managed or alarmed as specified in R2.	2.4	Niveau 4 : Les systèmes de télécommunications ne sont pas activement surveillés, vérifiés, gérés ou dotés de mécanismes d'alarme, contrairement à ce que prévoit l'exigence E2.
3.	Levels of Non-Compliance – NERCnet User Organization	3.	Niveaux de non-conformité – Organisation utilisatrice du NERCnet :
3.1	Level 1: Not applicable		Niveau 1 : Sans objet.
3.2	Level 2: Not applicable		Niveau 2 : Sans objet.
3.3	Level 3: Not applicable		Niveau 3 : Sans objet.
3.4	Level 4: Did not adhere to the requirements in Attachment 1-COM-001, NERCnet Security Policy.		Niveau 4 : Non-respect des exigences de l'annexe 1-COM-001, intitulée « Politique de sécurité relative au NERCnet ».

E. Regional Differences / Différences régionales

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

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised

Historique des versions

Version	Date	Intervention	Suivi des modifications
0	1er avril 2005	Date d'entrée en vigueur	Nouvelle norme
0	8 août 2005	Suppression de «proposée» de la date d'entrée en vigueur dans la version anglaise	Erratum
1	1 ^{er} novembre 2006	Adoptée par le Conseil d'administration	Mise à jour

Attachment 1-COM-001— NERCnet Security Policy	Annexe 1-COM-001— Politique de sécurité relative au NERCnet
<p>Policy Statement</p> <p>The purpose of this NERCnet Security Policy is to establish responsibilities and minimum requirements for the protection of information assets, computer systems and facilities of NERC and other users of the NERC frame relay network known as “NERCnet.”. The goal of this policy is to prevent misuse and loss of assets.</p> <p>For the purpose of this document, information assets shall be defined as processed or unprocessed data using the NERCnet Telecommunications Facilities including network documentation. This policy shall also apply as appropriate to employees and agents of other corporations or organizations that may be directly or indirectly granted access to information associated with NERCnet.</p> <p>The objectives of the NERCnet Security Policy are:</p> <ul style="list-style-type: none"> • To ensure that NERCnet information assets are adequately protected on a cost-effective basis and to a level that allows NERC to fulfill its mission. • To establish connectivity guidelines for a minimum level of security for the network. • To provide a mandate to all Users of NERCnet to properly handle and protect the information that they have access to in order for NERC to be able to properly conduct its business and provide services to its customers. 	<p>Énoncé de politique</p> <p>L’objet de la présente politique de sécurité relative à NERCnet est d’établir les responsabilités et les exigences minimales en vue de la protection des actifs informationnels, des systèmes et des installations informatiques de la NERC et des autres utilisateurs du réseau à relais de trames de la NERC désigné par le terme « NERCnet ». Le but de cette politique est de prévenir toute mauvaise utilisation des actifs informationnels ou leur perte.</p> <p>Aux fins du présent document, on entend par actifs informationnels l’ensemble des données brutes ou traitées employant les installations de télécommunications du NERCnet, y compris la documentation sur le réseau. Cette politique s’applique également, le cas échéant, aux employés et aux agents d’autres sociétés ou organismes auxquels peut être accordé directement ou indirectement un accès à l’information liée au NERCnet.</p> <p>Les objectifs de la politique de sécurité relative au NERCnet consistent à :</p> <ul style="list-style-type: none"> • obtenir l’assurance que les actifs informationnels du NERCnet sont protégés adéquatement, de manière économique, et à un niveau qui permet à la NERC de remplir sa mission. • établir des directives en matière de connectivité assurant un niveau minimum de sécurité pour le réseau. • donner à tous les utilisateurs du NERCnet le mandat de traiter et protéger convenablement l’information à laquelle ils ont accès de manière que la NERC puisse mener à bien ses affaires et desserve ses clients convenablement.
<p>NERC’s Security Mission Statement</p> <p>NERC recognizes its dependency on data, information, and the computer systems used to facilitate effective operation of its business and fulfillment of its mission. NERC also recognizes the value of the information maintained and provided to its members and others authorized to have access to NERCnet. It is, therefore, essential that this data, information, and computer systems, and the manual and technical infrastructure that supports it, are secure from destruction, corruption, unauthorized access, and accidental or deliberate breach of confidentiality.</p>	<p>Énoncé de la mission de la NERC en matière de sécurité</p> <p>La NERC reconnaît sa dépendance par rapport aux données, à l’information et aux systèmes informatiques employés pour faciliter la conduite efficace de ses affaires et l’accomplissement de sa mission. La NERC reconnaît également la valeur de l’information gérée et fournie à ses membres et aux autres intervenants autorisés à accéder au NERCnet. Par conséquent, il est essentiel que ces données, ces informations et ces systèmes informatiques ainsi que l’infrastructure manuelle et technique qui les soutiennent soient protégés de la destruction, de la corruption, des intrusions, des accès non autorisés et des violations de la confidentialité accidentelles ou délibérées.</p>
<p>Implementation and Responsibilities</p> <p>This section identifies the various roles and responsibilities related to the protection of NERCnet resources.</p>	<p>Mise en œuvre et responsabilités</p> <p>Cette section définit les divers rôles et responsabilités se rapportant à la protection des ressources du NERCnet.</p>

Attachment 1-COM-001— NERCnet Security Policy	Annexe 1-COM-001— Politique de sécurité relative au NERCnet
<p>NERCnet User Organizations</p> <p>Users of NERCnet who have received authorization from NERC to access the NERC network are considered users of NERCnet resources. To be granted access, users shall complete a User Application Form and submit this form to the NERC Telecommunications Manager.</p>	<p>Organisations utilisatrices du NERCnet</p> <p>Les utilisateurs du NERCnet qui ont reçu de la NERC l'autorisation d'accéder à son réseau sont considérés comme des utilisateurs des ressources du NERCnet. Pour obtenir un accès autorisé, les utilisateurs doivent remplir un formulaire de demande et le soumettre au gestionnaire des télécommunications de la NERC.</p>
<p>Responsibilities</p> <p>It is the responsibility of NERCnet User Organizations to:</p> <ul style="list-style-type: none"> • Use NERCnet facilities for NERC-authorized business purposes only. • Comply with the NERCnet security policies, standards, and guidelines, as well as any procedures specified by the data owner. • Prevent unauthorized disclosure of the data. • Report security exposures, misuse, or non-compliance situations via Reliability Coordinator Information System or the NERC Telecommunications Manager. • Protect the confidentiality of all user IDs and passwords. • Maintain the data they own. • Maintain documentation identifying the users who are granted access to NERCnet data or applications. • Authorize users within their organizations to access NERCnet data and applications. • Advise staff on NERCnet Security Policy. • Ensure that all NERCnet users understand their obligation to protect these assets. • Conduct self-assessments for compliance. 	<p>Responsabilités</p> <p>Il est de la responsabilité des organisations utilisatrices du NERCnet :</p> <ul style="list-style-type: none"> • d'utiliser les installations du NERCnet exclusivement pour les activités autorisées par la NERC ; • de se conformer aux politiques, normes et directives de sécurité relative au NERCnet ainsi qu'à toute procédure précisée par le propriétaire des données ; • de se prémunir contre la divulgation non autorisée de données ; • de déclarer les situations d'exposition à des risques de sécurité, les mauvaises utilisations et les cas de non-conformité par l'intermédiaire du système d'information des coordonnateurs de la fiabilité ou du gestionnaire des télécommunications de la NERC ; • de protéger la confidentialité de tous les codes d'accès et mots de passe des utilisateurs ; • de gérer les données qui leur appartiennent ; • de tenir à jour les registres d'identification des utilisateurs ayant un accès autorisé aux données ou aux applications du NERCnet ; • d'autoriser leurs utilisateurs à accéder aux données et aux applications du NERCnet ; • d'informer le personnel de la politique de sécurité relative au NERCnet ; • de s'assurer que tous les utilisateurs du NERCnet comprennent leur obligation de protéger ces actifs informationnels ; • d'effectuer des auto-évaluations de conformité.

Attachment 1-COM-001— NERCnet Security Policy	Annexe 1-COM-001— Politique de sécurité relative au NERCnet
<p>User Accountability and Compliance</p> <p>All users of NERCnet shall be familiar and ensure compliance with the policies in this document.</p> <p>Violations of the NERCnet Security Policy shall include, but not be limited to any act that:</p> <ul style="list-style-type: none"> • Exposes NERC or any user of NERCnet to actual or potential monetary loss through the compromise of data security or damage. • Involves the disclosure of trade secrets, intellectual property, confidential information or the unauthorized use of data. <p>Involves the use of data for illicit purposes, which may include violation of any law, regulation or reporting requirement of any law enforcement or government body.</p>	<p>Responsabilité et conformité des utilisateurs</p> <p>Tous les utilisateurs du NERCnet doivent être au fait des politiques énoncées dans le présent document et s’y conformer.</p> <p>Les violations à la politique de sécurité relative au NERCnet comprennent, sans s’y limiter, tout acte qui :</p> <ul style="list-style-type: none"> • expose la NERC ou tout utilisateur du NERCnet à des pertes pécuniaires réelles ou potentielles par la compromission de la sécurité des données ou tout autre préjudice ; • donne lieu à la divulgation de secrets commerciaux, de propriété intellectuelle ou d’information confidentielle ou à l’utilisation non autorisée de données ; • donne lieu à l’utilisation de données à des fins illicites, ce qui peut comprendre la violation d’une loi, d’un règlement ou d’une exigence de déclaration de tout organisme chargé de l’application de la loi ou de tout organisme gouvernemental.