

## A. Introduction

1. **Title:** **Telecommunications**
2. **Number:** COM-001-~~24~~
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.
4. **Applicability:**
  - 4.1. Transmission Operators.
  - 4.2. Balancing Authorities.
  - 4.3. Reliability Coordinators.
  - 4.4. Distribution Providers.
  - 4.5. Generator Operators.
  - ~~4.4. NERCNet User Organizations.~~
5. **Effective Date:** TBD ~~January 1, 2007~~

## B. Requirements

~~R1. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information:~~

~~R1.1. Internally.~~

~~R1.2. Between the Reliability Coordinator and its Transmission Operators and Balancing Authorities.~~

~~R1.3. With other Reliability Coordinators, Transmission Operators, and Balancing Authorities as necessary to maintain reliability.~~

~~R1.4. Where applicable, these facilities shall be redundant and diversely routed.~~

~~R2. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall operationally test, on a quarterly basis at a minimum, alternative manage, alarm, test and/or actively monitor vital telecommunications facilities to ensure the availability of their use when normal telecommunications facilities fail. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications. [Violation Risk Factor: Medium][Time Horizon: Real-time Operations]~~

~~R1.~~

~~R2. Each Reliability Coordinator, Transmission Operator and Balancing Authority shall notify impacted entities of the failure of its normal telecommunications facilities, and~~

The RC SDT contends that COM-001-1, R1 and its subrequirements are low level facilitating requirements that are more appropriately and inherently monitored under various higher-level performance-based reliability requirements for each entity throughout the body of standards. (See Implementation Plan for examples.)

~~shall verify that alternate means of telecommunications are functional. 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 *[Violation Risk Factor: Medium][Time Horizon: Real-time Operations]*~~

**R3.** Unless agreed to otherwise, each Reliability Coordinator, Transmission Operator, ~~and~~ Balancing Authority, Generator Operator and Distribution Provider shall use English as the language for all inter-entity Bulk Electric System (BES) reliability communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected ~~Bulk Electric System~~ BES. Transmission Operators and Balancing Authorities may use an alternate language for internal operations. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

Requirement R3 is being incorporated into COM-003-1 by the Operations Personnel Communications Protocols SDT (Project 2007-02). It will be retired from this standard upon approval of COM-003-1.

~~**R4.** 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.~~

The RC SDT is recommending that R4 be retired as it is redundant with EOP-008-0.

~~**R5.** Each NERCNet User Organization shall adhere to the requirements in Attachment 1 COM-001, "NERCNet Security Policy."~~

The RC SDT is recommending that R5 be retired. This is an ERO procedural issue and should not be in a reliability standard. It should be retired and included in the NERC Rules of Procedure.

**R4.** Each Distribution Provider and Generation Operator shall have telecommunications facilities with its Transmission Operator and Balancing Authority for the exchange of Interconnection and operating information. *[Violation Risk Factor: High][Time Horizon: Real-time Operations and Operations Planning]*

The new R4 was written to meet a FERC Directive from Order 693.

### C. Measures

~~**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.** Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide evidence that it operationally tested, on a quarterly basis at a minimum,

alternative telecommunications facilities to ensure the availability of their use when normal telecommunications facilities fail.

**M2.** Each Reliability Coordinator, Transmission Operator and Balancing Authority shall provide evidence that it notified impacted entities of failure of their normal telecommunications facilities, and verified the alternate means of telecommunications were functional.

**M3.** 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 that personnel used English as the language for all inter-entity BES reliability communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected BES compliance to Requirement 4.

~~**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.~~

~~**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.** Each Distribution Provider and Generation Operator has telecommunications facilities with its Transmission Operator and Balancing Authority for the exchange of Interconnection and operating information.

## D. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority

#### ~~1.1. Compliance Monitoring Responsibility~~

~~NERC shall be responsible for compliance monitoring of the Regional Entity Reliability Organizations~~

~~Regional Reliability Organizations shall be responsible for compliance monitoring of all other entities~~

#### 1.2. Compliance Monitoring and Enforcement Processes ~~Reset Time Frame~~

Compliance Audits

Self-Certifications

~~One or more of the following methods will be used to assess compliance:~~

~~— Self-certification (Conducted annually with submission according to schedule.)~~

- Spot ~~Checking~~ Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- ~~Compliance Violation~~ 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.)

### Self-Reporting

### Complaints

~~The Performance Reset Period shall be 12 months from the last finding of non-compliance.~~

## 1.3. Data Retention

~~The~~ For Measure 1 each Reliability Coordinator, Transmission Operator and, Balancing Authority shall keep data or evidence to show of compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

For the Measures, ~~previous two calendar years plus the current year.~~

~~For Measure 2~~ each Reliability Coordinator, Transmission Operator, and Balancing Authority shall each keep the most recent three months ~~90 days~~ of historical data (evidence).

~~If a~~ For Measure 3, each Reliability Coordinator, Transmission Operator and, Balancing Authority ~~shall have its current operating instructions and procedures to confirm that it meets Requirement 5.~~

~~For Measure 4,~~ each Reliability Coordinator, Transmission Operator, Balancing Authority and NERC ~~net User Organization shall keep 90 days of historical data (evidence).~~

~~If an entity~~ is found non-compliant it the entity shall keep information related to the noncompliance until found compliant, ~~or for two years plus the current year, whichever is longer.~~

~~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.~~

The Compliance Enforcement Authority ~~Monitor~~ shall keep the last periodic ~~audit records~~ report and all requested and submitted subsequent audit ~~compliance~~ records.

**1.4. Additional Compliance Information**

None

2. Violation Severity Levels

<u>Requirement</u>	<u>Lower VSL</u>	<u>Moderate VSL</u>	<u>High VSL</u>	<u>Severe VSL</u>
<u>R1</u>	<u>The Reliability Coordinator, Transmission Operator, or Balancing Authority failed to operationally test within the last quarter.</u>	<u>The Reliability Coordinator, Transmission Operator, or Balancing Authority failed to operationally test within the last 2 quarters.</u>	<u>The Reliability Coordinator, Transmission Operator, or Balancing Authority failed to operationally test within the last 3 quarters.</u>	<u>The Reliability Coordinator, Transmission Operator, or Balancing Authority failed to operationally test within the last 4 quarters.</u>
<u>R2</u>	<u>The Reliability Coordinator, Transmission Operator or Balancing Authority notified all impacted entities of the failure of their normal telecommunications facilities, but failed to verify the alternate means of telecommunications are functional.</u>	<u>The Reliability Coordinator, Transmission Operator or Balancing Authority notified some, but not all, impacted entities of the failure of their normal telecommunications facilities, and failed to verify the alternate means of telecommunications are functional.</u>	<u>N/A</u>	<u>The Reliability Coordinator, Transmission Operator or Balancing Authority failed to notify any impacted entities of the failure of their normal telecommunications facilities, and failed verify the alternate means of telecommunications are functional.</u>

<u>Requirement</u>	<u>Lower VSL</u>	<u>Moderate VSL</u>	<u>High VSL</u>	<u>Severe VSL</u>
<u>R3</u>	<u>N/A</u>	<u>N/A</u>	<u>N/A</u>	<p><u>The responsible entity failed to provide evidence of concurrence to use a language other than English for all communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected Bulk Electric System.</u></p>
<u>R4</u>	<u>N/A</u>	<u>N/A</u>	<u>N/A</u>	<p><u>The Distribution Provider or Generation Operator failed to have telecommunications facilities with its Transmission Operator and Balancing Authority</u></p>

Attachment 1 COM-001 — NERCnet Security Policy

- ~~2. **Levels of Non-Compliance for Transmission Operator, Balancing Authority or Reliability Coordinator**~~
  - ~~2.1. **Level 1:** Not applicable.~~
  - ~~2.2. **Level 2:** Not applicable.~~
  - ~~2.3. **Level 3:** There shall be a separate Level 3 non-compliance, for every one of the following requirements that is in violation:
 
    - ~~2.3.1 The Transmission Operator, Balancing Authority or Reliability Coordinator used a language other than English without agreement as specified in R4.~~
    - ~~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.~~~~
  - ~~2.4. **Level 4:** Telecommunication systems are not actively monitored, tested, managed or alarmed as specified in R2.~~
- ~~3. **Levels of Non-Compliance — NERCnet User Organization**~~
  - ~~3.1. **Level 1:** Not applicable.~~
  - ~~3.2. **Level 2:** Not applicable.~~
  - ~~3.3. **Level 3:** Not applicable.~~
  - ~~3.4. **Level 4:** Did not adhere to the requirements in Attachment 1 COM-001, NERCnet Security Policy.~~

**E. Regional Differences**

None identified.

**F. Associated Documents**

None Identified.

**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
<u>1</u>	<u>April 4, 2007</u>	<u>Regulatory Approval — Effective Date</u>	<u>New</u>
<u>1</u>	<u>April 6, 2007</u>	<u>Requirement 1, added the word “for”</u>	<u>Errata</u>



**Standard COM-001-1 — Telecommunications**

---

		<u>between “facilities” and “the exchange.”</u>	
<u>2</u>	<u>TBD</u>	<u>Revised per SAR for Project 2006-06, RCSDT</u>	<u>Revised</u>

## **Attachment 1-COM-001 — NERCnet Security Policy**

### **Policy Statement**

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.

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.

The objectives of the NERCnet Security Policy are:

- 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.

### **NERC’s Security Mission Statement**

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.

### **Implementation and Responsibilities**

———— This section identifies the various roles and responsibilities related to the protection of NERCnet resources.

#### **NERCnet User Organizations**

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.

#### **Responsibilities**

It is the responsibility of NERCnet User Organizations to:

- 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.~~
- ~~User Accountability and Compliance~~
- ~~All users of NERCnet shall be familiar and ensure compliance with the policies in this document.~~
- ~~Violations of the NERCnet Security Policy shall include, but not be limited to any act that:~~
- ~~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.~~
- ~~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.~~