Standard COM-001-2 — Telecommunications

Requirement R4 was assigned to Project 2007-02. All other requirements were assigned to Project 2006-06 and are being revised or retired under Project 2006-06.

A. Introduction

1. **Title:** **Telecommunications**
2. **Number:** COM-001-2
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.** NERCNet User Organizations.
5. **(Proposed) Effective Date:** First day of the first calendar quarter, six calendar months following applicable regulatory approval; or, in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter a year from the date of Board of Trustee adoption.

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 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.

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.

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.

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

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)

M2. 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 4.

M3. 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 5)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

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

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

1.2. Compliance Monitoring and Reset Time Frame

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

- 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.)

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

1.3. Data Retention

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.

For Measure 2, each Reliability Coordinator, Transmission Operator, Balancing Authority shall have its current operating instructions and procedures to confirm that it meets Requirement 4.

For Measure 3, each Reliability Coordinator, Transmission Operator, Balancing Authority and NERCnet User Organization shall keep 90 days of historical data (evidence).

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.

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 Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

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 There are no written operating instructions and procedures to enable continued operation of the system during the loss of telecommunication facilities, as specified in R4.

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.

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
1	April 6, 2007	Requirement 1, added the word “for” between “facilities” and “the exchange.”	Errata
1.1	October 29, 2008	BOT adopted errata changes; updated version number to “1.1”	Errata

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.