A. Introduction

1. Title: **Telecommunications**

2. Number: COM-001-0

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. Effective Date: April 1, 2005

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. 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.

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.

R6. Each NERCNet User Organization shall adhere to the requirements in Attachment 1-COM-001-0, "NERCNet Security Policy."

C. Measures

Not Specified.

D. Compliance

Not specified.

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
0	October 3, 2005	Added “for” between “facilities” and “the” in Requirement 1.	Errata

Attachment 1-COM-001-0 — 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.