NORTHEAST UTILITIES
COMPLIANCE PLAN
IMPLEMENTING FERC ORDER NO. 717
STANDARDS OF CONDUCT FOR TRANSMISSION PROVIDERS

TABLE OF CONTENTS

Appendices:

A. Northeast Utilities (NU) System Corporate Chart
B. Affiliate Transaction Principles
C. Affiliate Rules: Codes of Conduct for Regulated and Marketing Affiliates
D. Training Materials
E. Corporate Information Security Department Processes
F. Confidential Information Policies
G. New England Power Pool (NEPOOL) Information Policy

THE NORTHEAST UTILITIES SYSTEM
COMPLIANCE PLAN
IMPLEMENTING FERC ORDER NO. 717
STANDARDS OF CONDUCT FOR TRANSMISSION PROVIDERS

INTRODUCTION

Northeast Utilities Service Company ("NUSCO" or "the Company") on behalf of its parent, Northeast Utilities ("NU"), and its operating company affiliates, The Connecticut Light and Power Company ("CL&P"), Western Massachusetts Electric Company ("WMECO"), NSTAR Electric Company ("NSTAR") and Public Service Company of New Hampshire ("PSNH") (hereinafter referred to collectively as the "NU Companies"), provides this updated version of the Compliance Plan (the "Plan") in adherence with Part 358.7(d) of the Federal Energy Regulatory Commission (the "FERC" or "Commission") Standards of Conduct for Transmission Providers (the "Standards" or "Code" or the "Standards of Conduct") and FERC Order No. 717.[1]

The NU Companies are wholly owned subsidiaries of NU, a registered holding company under the Public Utility Holding Company Act of 2005, and are classified as Transmission Providers, as that term is described in Part 358.3(k), of the Commission's regulations.

In sections A through D of this introduction to this Plan, NU summarizes several compliance mechanisms and guidelines that are central to NU's Code-related activities. The Plan follows and presents a section-by-section listing and discussion of procedures and mechanisms that the Company has developed to ensure compliance with the

[1] *Standards of Conduct for Transmission Providers*, Order No. 717, 125 FERC ¶ 61,064 (2008). 73 Fed. Reg. 63796 (Oct. 27, 2008)(referred to herein as "FERC Order No.717").

Standards. More detailed descriptions of training and policy materials follow the Compliance Plan as appendices.

A. THE NU ORGANIZATION

NU's subsidiaries include a service company (NUSCO); four FERC rate-regulated electric utility operating companies (the NU Companies); a natural gas businesses holding company (Yankee Energy System, Inc.) that owns Yankee Gas Services Company and NSTAR Gas Company (both local gas distribution companies, and Hopkinton LNG Corp., a Hinshaw-exempt pipeline providing storage, liquefaction, and vaporization services to NSTAR Gas Company); a transmission holding company (NU Transmission Ventures, Inc.) that owns two transmission-related affiliates (Northern Pass Transmission, LLC, a planned participant-funded project, and Renewable Properties, Inc.); an unregulated businesses holding company (NU Enterprises, Inc., or NUEI) that owns an electric generation services company (Northeast Generation Services Company, which in turn wholly owns E.S. Boulos Company) and one telecommunications company (NSTAR Communications, Inc.); and two real estate companies (the HWP Company and The Rocky River Realty Company). Other NU subsidiaries are shown on the NU System Corporate Chart in Appendix A.

NU and its subsidiaries are referred to collectively herein as the "NU System." A copy of the NU System Corporate Chart listing and describing all of the NU System companies is included as Appendix A to this compliance filing.

B. THE CORPORATE COMPLIANCE DEPARTMENT

The NU System has operated under a variety of affiliate standards and codes of conduct since 1997.[2] The Northeast Utilities Service Company ("NUSCO") Corporate Compliance Department was established to implement and administer the various codes of conduct to which the NU System companies are subject. The Corporate Compliance Manager reports to NU's Deputy General Counsel and Chief Compliance Officer. The NU Deputy General Counsel and Chief Compliance Officer has been designated as the FERC Chief Compliance Officer, as required in § 358.8(c)(2) of the Commission's regulations.

NUSCO's Corporate Compliance department is principally supported by the NU Legal, Human Resources, Corporate Communications, Information Technology, Rates and Revenue Requirements, Facilities, Security and Transmission department personnel. The Corporate Compliance Manager provides education, direction, and oversight to all NU subsidiaries on matters related to understanding and implementing the standards of conduct. The Corporate Compliance Manager also facilitates the timely documentation

[2] *Open Access Same-Time Information System (Formerly Real-Time Information Network) and Standards of Conduct,* Order No. 889, 61 FR 21737 (May 10, 1996), FERC Stats. & Regs., Regulations Preambles January 1991 – June 1996 ¶ 31,035 (1996); Order No. 889-A, *order on reh'g*, 62 FR 12484 (Mar. 14, 1997), FERC Stats. & Regs., Regulations Preambles July 1996 – December 2000 ¶ 31,049 (1997); Order No. 889-B, *reh'g denied*, 62 FR 64715 (Dec. 9, 1997), 81 FERC ¶ 61,253 (1997) (collectively, Order No. 889). The NU Companies Order No. 889 Standards of Conduct were initially filed with the Commission on December 31, 1996 and became effective January 3, 1997. S*ee, Illinois Power Co.,* 81 FERC ¶ 61,338 (1997)*; Allegheny Power Service Corp.* 84 FERC ¶ 61,124 (1998), 85 FERC ¶ 61,390 (1998). Retail competition codes of conduct were adopted in each of the states in which the NU Companies provide distribution service beginning in 1998. *Standards of Conduct for Transmission Providers,* Order No. 2004, FERC Stats. & Regs., Regulations Preambles 2001 – 2005 ¶ 31,155 (2003); o*rder on Reh'g*, Order No. 2004-A, FERC Stats.& Regs., Regulations Preambles 2001 – 2005 ¶ 31,161 (2004); o*rder on Reh'g,* Order No. 2004-B, FERC Stats. & Regs., Regulations Preambles 2001 – 2005 ¶ 31,166 (2004); *order on reh'g,* Order No. 2004-C, FERC Stats. & Regs., Regulations Preambles 2001 – 2005 (2004); order on reh'g, Order No. 2004-D, 110 FERC ¶ 61,320 (2005), *vacated and remanded as it applies to natural gas pipelines sub nom. Nat'l Fuel Gas Supply Corp. v. FERC*, 468 F.3d 831 (D.C. Cir. 2006) (collectively referred to herein as "FERC Order No. 2004").

and reporting of affiliate transactions via the OASIS and NU Internet Web sites and files Compliance Plans as required in some states.

The Corporate Compliance Manager is responsible for addressing affiliate rules issues and directing company-wide efforts to comply with federal and state regulations. Some of the tools utilized include intranet access to all codes of conduct, the training discussed below and general training materials provided directly to employees on request.

C. TRAINING AND COMMUNICATIONS

An ongoing education and training program is the primary means for ensuring compliance with the federal and state affiliate rules. Mandatory affiliate rules training is held throughout the NU System. At the core of this program are these principles:

- NU's business structure is maintained to ensure that NU transmission, distribution and gas business segments or companies are in full compliance with all applicable state and federal codes of conduct,
- prohibitions on information sharing, restrictions on employee transfers, and physical separation requirements, and
- regulated businesses must act in a nondiscriminatory fashion in their interactions with marketing affiliates.

Both written and electronic media are also used to enhance employee knowledge of the regulations and corporate policies and procedures for ensuring compliance.

A Lotus Notes database, entitled "Regulatory Compliance Coordinator Library", is also available to all employees and includes topics related to:

- Code of Conduct-related presentations
- Training administration
- State Rules

- FERC Order No. 717
- Affiliate Transaction Principles (Appendix B)

NU administers a NUnet internal Web site containing the "Code of Business Conduct" (the "Code"). The Web site provides convenient, user friendly on-line links to related policies and procedures. The Web site contains the ethical and legal principles that must be followed by everyone working within the NU system. The Code is an integral part of NU's Corporate Compliance Program and applies to all trustees, directors, officers, employees, contractors and agents of NU System companies. Topics addressed in the Code include, among other things, the following:

- Affiliate Rules
- Conflicts of Interest
- Environmental Responsibility
- Employee Conduct

The Code was also designed to address a variety of topics, such as workplace interactions, accountability and personal conduct. The Code succinctly outlines behavioral expectations and provides information on ethical decision making. The Code is also available on the NU external Web site and at all Area Work Centers to ensure full access for employees from any internet connection.

NU also maintains relevant internal Policies and Procedures in a central database and Web site entitled "Policies, Procedures and Manuals" located on the NU internal internet. These documents are placed in central office locations as an accessible resource for all employees.

The "Policies, Procedures and Manuals" section includes "Affiliate Rules" information. This area affords employees the opportunity to choose topics from the available Procedures, Resources (actual codes of conduct), or Contacts options. These menu options display detailed information regarding affiliate transaction rules.

NU's state regulated operating companies (PSNH, CL&P, WMECO, Yankee Gas, NSTAR Gas and NSTAR Electric) and transmission business segment also administer a "Regulated Businesses Policies and Procedures" database. Employees can access all group policies and procedures via either a Lotus Notes Database or the Company Intranet. The database supports unit-specific, company, and enterprise-wide policies, procedures or guidelines by electronically linking regulated businesses employees to the most current and latest approved version of the document. The database eliminates the need for physical "hard copy" storage and allows for annual or periodic reviews. Another feature of the database is that it serves as a portal to documents on enterprise-wide servers such as the NUnet.

The "Regulated Businesses Policies and Procedures" database provides a well-organized library of unified policies, procedures, and guidelines that is easily accessible to the vast majority of Regulated Business employees. In general, the database accomplishes the following internal control objectives:

- Identifies ownership of existing policies and procedures
- Archives existing policies and procedures without owners
- Creates an efficient process for future additions, deletions, or revisions to the policies and procedures
- Organizes and indexes policies and procedures in one library where they can be easily accessed by employees
- Makes information available for future use, including training and educational activities

The orientation process for newly-hired employees includes references to Code of Conduct materials. Each new employee receives an information packet that includes, among other things, a tri-fold brochure that summarizes the NU Procedure "Affiliate Rules: Codes of Conduct for Regulated and Marketing Affiliates" (Appendix C). This

document is also included in the offer letter sent to prospective new employees. Copies of all codes of conduct are currently available to employees via the NU intranet.

NU recognizes that many NU System employees are physical workers without ready access to the Company's e-mail or Intranet systems. As a result, Company-wide employee communications are generally distributed as an NU Today Extra publication with the following message attached: "Please be sure to post this in a prominent place or distribute to employees who do not have access to a computer."

To satisfy the specific training requirements detailed in FERC Order No. 717, Standards of Conduct for Transmission Providers, all NU functional groups utilize a computer-based training module offered by the Edison Electric Institute (EEI)(Appendix D). The training is administered annually. The EEI training was developed in conjunction with Skadden, Arps, Slate, Meagher & Flom LLP. The training module provides on-line training related to all aspects of the FERC Order No. 717 rules. The FERC Order No. 717 affiliate rules requirements and the related training are similar in certain areas and in certain respects more restrictive than the Affiliate Transactions Rules.

D. COMPLIANCE PLAN PROCEDURES AND MECHANISMS

A number of mechanisms, policies and procedures created to ensure compliance with FERC Order No. 717 and the State codes reside in various departments throughout the NU System. Those compliance measures are referred to in this Compliance Plan and are included in appendices where appropriate.

NORTHEAST UTILITIES
WRITTEN PROCEDURES
IMPLEMENTING FERC ORDER NO. 717
STANDARDS OF CONDUCT FOR TRANSMISSION PROVIDERS

SUBCHAPTER S -- STANDARDS OF CONDUCT FOR TRANSMISSION PROVIDERS

Part 358 -- STANDARDS OF CONDUCT

Sec.

Authority: 15 U.S.C. 717–717w, 3301–3432; 16 U.S.C. 791–825r, 2601–2645; 31 U.S.C. 9701; 42 U.S.C. 7101–7352.

§ 358.1 Applicability.

(a) This part applies to any interstate natural gas pipeline that transports gas for others pursuant to subparts B or G of part 284 of this chapter and conducts transmission transactions with an affiliate that engages in marketing functions.

(b) This part applies to any public utility that owns, operates, or controls facilities used for the transmission of electric energy in interstate commerce and conducts transmission transactions with an affiliate that engages in marketing functions.

(c) This part does not apply to a public utility transmission provider that is a Commission-approved Independent System Operator (ISO) or Regional Transmission Organization (RTO). If a public utility transmission owner participates in a Commission-approved ISO or RTO and does not operate or control its transmission system and has no access to transmission function information, it may request a waiver from this part.

(d) A transmission provider may file a request for a waiver from all or some of the requirements of this part for good cause.

Procedures and Mechanisms for Ensuring Compliance

The Connecticut Light & Power Company (CL&P), Western Massachusetts Electric Company (WMECO), NSTAR Electric Company (NSTAR) and Public Service Company of New Hampshire (PSNH) are wholly-owned subsidiaries of Northeast Utilities ("NU"), a registered holding company under the Public Utility Holding

Company Act of 1935. CL&P, WMECO, NSTAR and PSNH are classified as Transmission Providers, as that term is described in § 358.3, Definitions.

* * * * *

§ 358.2 General principles.

(a) A transmission provider must treat all transmission customers, affiliated and non-affiliated, on a not unduly discriminatory basis, and must not make or grant any undue preference or advantage to any person or subject any person to any undue prejudice or disadvantage with respect to any transportation of natural gas or transmission of electric energy in interstate commerce, or with respect to the wholesale sale of natural gas or of electric energy in interstate commerce.

Procedures and Mechanisms for Ensuring Compliance

A significant portion of the computer-based training program focuses on nondiscrimination and non-preferential treatment standards required by the Code.

* * * * *

(b) A transmission provider's transmission function employees must function independently from its marketing function employees, except as permitted in this part or otherwise permitted by Commission order.

Procedures and Mechanisms for Ensuring Compliance

Measures adopted to ensure compliance with this section of the Code involve corporate and business unit separation, functional separation, information technology separation and physical separation of the Transmission Function Employees from the Marketing Function Employees. These activities are discussed in considerable detail in § 358.5(a), Independent Functioning Rule, in this filing.

A significant portion of the NU education and training program focuses on the functional independence standards required by Order No. 717. Relevant training materials have been developed that describe the FERC Order No. 717 separation rules and OASIS posting requirements. Topics discussed include:

- independent functioning
- nondiscrimination and non-preferential treatment standards
- prohibition against affiliates conducting transmission operations or having access to control center or similar facilities
- prohibitions regarding Transmission Provider system information access

- anti-conduit rules regarding information sharing
- application of tariff provisions

* * * * *

(c) A transmission provider and its employees, contractors, consultants and agents are prohibited from disclosing, or using a conduit to disclose, non-public transmission function information to the transmission provider's marketing function employees.

Procedures and Mechanisms for Ensuring Compliance

NU training materials explain the prohibition against a Transmission Provider using anyone as a conduit to inappropriately share information with a Marketing Function Employee.

* * * * *

(d) A transmission provider must provide equal access to non-public transmission function information to all its transmission function customers, affiliated and non-affiliated, except in the case of confidential customer information or Critical Energy Infrastructure Information.

Procedures and Mechanisms for Ensuring Compliance

The EEI training materials explain that a transmission provider must provide equal access to non-public transmission function information its transmission function customers.

* * * * *

§ 358.3 Definitions.

(a) Affiliate of a specified entity means:
(1) Another person that controls, is controlled by or is under common control with, the specified entity. An affiliate includes a division of the specified entity that operates as a functional unit.
(2) For any exempt wholesale generator (as defined under § 366.1 of this chapter), affiliate shall have the meaning set forth in § 366.1 of this chapter, or any successor provision.
(3) "Control" as used in this definition means the direct or indirect authority, whether acting alone or in conjunction with others, to direct or cause to direct the management policies of an entity. A voting interest of 10 percent or more creates a rebuttable presumption of control.

(b) Internet website refers to the Internet location where an interstate natural gas pipeline or a public utility posts the information, by electronic means, required under this part 358.

(c) Marketing functions means:
(1) in the case of public utilities and their affiliates, the sale for resale in interstate commerce, or the submission of offers to sell in interstate commerce, of electric energy or capacity, demand response, virtual transactions, or financial or physical transmission rights, all as subject to an exclusion for bundled retail sales, including sales of electric energy made by providers of last resort (POLRs) acting in their POLR capacity; and
(2) in the case of interstate pipelines and their affiliates, the sale for resale in interstate commerce, or the submission of offers to sell in interstate commerce, natural gas, subject to the following exclusions:

(i) Bundled retail sales,
(ii) Incidental purchases or sales of natural gas to operate interstate natural gas pipeline transmission facilities,
(iii) Sales of natural gas solely from a seller's own production,
(iv) Sales of natural gas solely from a seller's own gathering or processing facilities, and
v) Sales by an intrastate natural gas pipeline, by a Hinshaw interstate pipeline exempt from the Natural Gas Act, or by a local distribution company making an on-system sale.

(d) Marketing function employee means an employee, contractor, consultant or agent of a transmission provider or of an affiliate of a transmission provider who actively and personally engages on a day-to-day basis in marketing functions.

(e) Open Access Same Time Information System or OASIS refers to the Internet location where a public utility posts the information required by part 37 of this chapter, and where it may also post the information required to be posted on its Internet website by this part 358.

(f) Transmission means electric transmission, network or point-to-point service, ancillary services or other methods of electric transmission, or the interconnection with jurisdictional transmission facilities, under part 35 of this chapter; and natural gas transportation, storage, exchange, backhaul, or displacement service provided pursuant to subparts B or G of part 284 of this chapter.

(g) Transmission customer means any eligible customer, shipper or designated agent that can or does execute a transmission service agreement or can or does receive transmission service, including all persons who have pending requests for transmission service or for information regarding transmission.

(h) Transmission functions means the planning, directing, organizing or carrying out of day-to-day transmission operations, including the granting and denying of transmission service requests.

(i) Transmission function employee means an employee, contractor, consultant or agent of a transmission provider who actively and personally engages on a day-to-day basis in transmission functions.

(j) Transmission function information means information relating to transmission functions.

(k) Transmission provider means:

(1) Any public utility that owns, operates or controls facilities used for the transmission of electric energy in interstate commerce; or
(2) Any interstate natural gas pipeline that transports gas for others pursuant to subparts B or G of part 284 of this chapter.
(3) A transmission provider does not include a natural gas storage provider authorized to charge market-based rates.

(l) Transmission service means the provision of any transmission as defined in § 358.3(f).

(m) Waiver means the determination by a transmission provider, if authorized by its tariff, to waive any provisions of its tariff for a given entity.

Procedures and Mechanisms for Ensuring Compliance

The Company has interpreted the term "Transmission Provider" to include the NU Companies CL&P, WMECO, NSTAR and PSNH. The "Transmission Function" refers to certain departments that perform transmission functions within these companies.

The term "Transmission Function Employee" refers to specific personnel within the Transmission Function who are actively and personally engaged on a day-to-day basis in transmission function activities.

The term "Marketing Function" includes certain personnel, actively and personally engaged on a day-to-day basis in marketing functions, employed in the following corporate entities or functional groups within Northeast Utilities:

> NUSCO's Wholesale Power Supply group within the Energy Supply department, which provides power sales and procurement services for CL&P, WMECO, NSTAR and PSNH on behalf of their retail load obligations.

* * * * *

§ 358.4 Non-discrimination requirements.

(a) A transmission provider must strictly enforce all tariff provisions relating to the sale or purchase of open access transmission service, if the tariff provisions do not permit the use of discretion.

(b) A transmission provider must apply all tariff provisions relating to the sale or purchase of open access transmission service in a fair and impartial manner that treats all transmission customers in a not unduly discriminatory manner, if the tariff provisions permit the use of discretion.

(c) A transmission provider may not, through its tariffs or otherwise, give undue preference to any person in matters relating to the sale or purchase of transmission service (including, but not limited to, issues of price, curtailments, scheduling, priority, ancillary services, or balancing).

(d) A transmission provider must process all similar requests for transmission in the same manner and within the same period of time.

Procedures and Mechanisms for Ensuring Compliance

Effective February 1, 2005, the NU Companies became participating transmission owners in the ISO New England ("ISO-NE") Regional Transmission Organization. ISO-NE administers a regional open access transmission tariff for New England. In addition, the NU Companies work very closely with ISO-NE in administering transmission service over their local networks in accordance with the ISO-NE Open Access Transmission Tariff, in order to provide transmission service that supports the competitive energy market in New England. Moreover, the NU Companies have complied with the Order No. 2004 non-discrimination requirements with respect to tariff administration and will continue such practices. All tariff provisions are applied in a nondiscriminatory manner and, if a tariff provision allows for discretion in its application, then the Transmission Provider will apply that tariff provision in the same manner to its Marketing Function affiliates as it does to all other transmission service customers.

Training materials note that Transmission Providers must treat all transmission customers, affiliated and non-affiliated, on a non-discriminatory manner.

* * * * *

§ 358.5 Independent functioning rule.

(a) General rule. Except as permitted in this part or otherwise permitted by Commission order, a transmission provider's transmission function employees must function independently of its marketing function employees.

Procedures and Mechanisms for Ensuring Compliance

Measures adopted to ensure compliance with this section of the Code involve Corporate and Business Unit Separation, Functional Separation of Employees, Physical Separation Measures, and Information Technology Separation measures. These activities are discussed separately below.

a. Corporate and Business Unit Separation

Transmission operations and wholesale marketing operations are conducted in separate business units within NUSCO, the service company supporting the NU Companies. Each business unit operates with its own budget and employees are not shared between business units.

b. Functional Separation of Employees

Employees who are engaged in transmission or distribution operations functions do not perform wholesale or retail marketing functions and are functionally separate from those employees. FERC Order No. 717 training materials describe the Transmission Provider prohibitions associated with permitting Marketing Function Employees from: 1) conducting transmission system operations or reliability functions, and 2) accessing system control centers or similar facilities used for transmission operations or reliability functions. Employees performing shared administrative or corporate support services are instructed to strictly account for time and resources spent on services provided to these functional areas and are instructed not to serve as conduits of non-public transmission or distribution information obtained through their work supporting the transmission and distribution operations functions to wholesale or retail marketing employees.

c. Physical Separation Measures

Employees who are engaged in transmission functions are also physically separated from marketing function employees. NU marketing function employees and its transmission function employees share two locations, but are physically separated at those locations. At the NU Corporate Center located at 107 Selden Street, Berlin, Connecticut 06037, marketing function employees are located in a separate building on the NU campus from the employees of CONVEX (the Connecticut Valley Electric Exchange), a scheduling and central dispatch local control center operating under the direction of ISO New England that coordinates the generation and transmission facilities of entities serving the electric needs of all of Connecticut and Western Massachusetts. Access to CONVEX offices is restricted via key card access to employees of CONVEX and NU involved in performing transmission reliability and operations functions.

NU marketing function employees and transmission function employees also share an office building located at One NSTAR Way, Westwood, Massachusetts 02090. All transmission function employees at this location are located on a separate floor from marketing function employees and access to that floor is restricted via key card access in order to prevent marketing function employees from gaining access.

Other NU transmission function employees, including those responsible for administering the NU OASIS, are located at 56 Prospect Street, Hartford, CT 06103. No marketing function employees operate from this location and access to the facility is restricted via keycard access.

The NSTAR Local Control Center, which performs functions similar to CONVEX for the eastern Massachusetts area under the direction of ISO New England, is located at a completely different physical location than the other NU offices. Access to the control center is restricted via key card access to employees of NU involved in performing transmission reliability and operations functions. Computer databases for the transmission function at the control center are password protected and are separate from those for the marketing function employees.

The Electric System Control Center (ESCC) is the New Hampshire Local Control Center that is responsible for the operation of transmission, distribution, and generating facilities under the direction of ISO New England, and is also the SCADA control center for PSNH. The ESCC is located at a different physical location than the other NU offices.

d. Information Technology Separation Measures

NU's information protection program requires all information stored and processed on corporate technology systems to be protected by default and each user that is granted access to be individually identified with strong password policies. Any access granted, whether to applications or specific data, requires a properly approved and documented access request. NU uses "best of breed" security technology to protect and monitor their systems and our program is regularly audited and tested to ensure effective on-going operation. In addition, computer databases for the Transmission Functions of NSTAR Electric are password protected and are separate from the computer databases for the Marketing Functions.

* * * * *

(b) Separation of functions.

(1) A transmission provider is prohibited from permitting its marketing function employees to:

(i) Conduct transmission functions; or
(ii) Have access to the system control center or similar facilities used for transmission operations that differs in any way from the access available to other transmission customers.

Procedures and Mechanisms for Ensuring Compliance

The compliance measures detailed in § 358.5(a), Independent functioning rule, describe the mechanisms adopted to ensure that Marketing Function Employees cannot perform transmission system activities or access system control centers or similar facilities.

FERC Order No. 717 training materials describe the Transmission Provider prohibitions associated with permitting Marketing Function Employees from: 1)

conducting transmission system operations or reliability functions, and 2) accessing system control centers or similar facilities used for transmission operations or reliability functions.

* * * * *

(2) A transmission provider is prohibited from permitting its transmission function employees to conduct marketing functions.

Procedures and Mechanisms for Ensuring Compliance

The prohibition against transmission function employees from conducting marketing functions is explained in the EEI training module on FERC Order No. 717. In addition, the physical and IT separation of Transmission Function and Marketing Function employees is maintained by the NU Security Department and the Corporate Compliance Manager.

* * * * *

§ 358.6 No conduit rule.

(a) A transmission provider is prohibited from using anyone as a conduit for the disclosure of non-public transmission function information to its marketing function employees.

(b) An employee, contractor, consultant or agent of a transmission provider, and an employee, contractor, consultant or agent of an affiliate of a transmission provider that is engaged in marketing functions, is prohibited from disclosing non-public transmission function information to any of the transmission provider's marketing function employees.

Procedures and Mechanisms for Ensuring Compliance

NU training materials explain the prohibition against a Transmission Provider using anyone as a conduit to inappropriately share information with Marketing Function personnel.

* * * * *

§ 358.7 Transparency rule.

(a) Contemporaneous disclosure.

(1) If a transmission provider discloses non-public transmission function information, other than information identified in paragraph (a)(2) of this section, in a manner contrary to the requirements of § 358.6, the transmission provider must immediately post the information that was disclosed on its Internet website.

(2) If a transmission provider discloses, in a manner contrary to the requirements of § 358.6, non-public transmission customer information, critical energy infrastructure information (CEII) as defined in § 388.113(c)(1) of this chapter or any successor provision, or any other information that the Commission by law has determined is to be subject to limited dissemination, the transmission provider must immediately post notice on its website that the information was disclosed.

Procedures and Mechanisms for Ensuring Compliance

Should an employee inadvertently disclose any information subject to the information disclosure and sharing restrictions described in Sections 358.6(a) and (b), the NU Transmission Provider will contemporaneously post that information on a NU Transmission Web page specifically designated for this purpose. This includes any other information referred to in Section 358.7(a)(2).

* * * * *

(b) Exclusion for specific transaction information. A transmission provider's transmission function employee may discuss with its marketing function employee a specific request for transmission service submitted by the marketing function employee. The transmission provider is not required to contemporaneously disclose information otherwise covered by § 358.6 if the information relates solely to a marketing function employee's specific request for transmission service.

Procedures and Mechanisms for Ensuring Compliance

As noted in § 358.5(a), Independent functioning rule, NU Transmission Providers maintain a number of policies and procedures regarding the handling of proprietary and confidential information. Appendix F displays some of those NU System-wide policies and procedures. Appendix G contains the New England Power Pool (NEPOOL) Information Policy. The NEPOOL Information Policy provides rules and guidelines regarding the appropriate disclosure of all information received, created and distributed in connection with the operation of and participation in NEPOOL, the stakeholder body for participants in the New England wholesale market.

NU has included in its Standards of Conduct training materials a discussion of the prohibitions on the Transmission Provider from: 1) disclosing to its Marketing Function Employees information concerning the transmission system of the Transmission Provider or the transmission system of another, or 2) sharing any information, acquired from nonaffiliated transmission customers or potential nonaffiliated transmission customers, or developed in the course of responding to requests for transmission or ancillary service on the OASIS or Internet website, with its Marketing Function Employees.

* * * * *

(c) Voluntary consent provision. A transmission customer may voluntarily consent, in writing, to allow the transmission provider to disclose the transmission customer's non-public information to the transmission provider's marketing function employees. If the transmission customer authorizes the transmission provider to disclose its information to marketing function employees, the transmission provider must post notice on its Internet website of that consent along with a statement that it did not provide any preferences, either operational or rate-related, in exchange for that voluntary consent.

Procedures and Mechanisms for Ensuring Compliance

The Company's training materials inform employees that Transmission Providers cannot provide customer information to its Marketing Function Employees, unless it has received written consent from the unaffiliated customer at issue.

Should a NU Transmission Provider obtain authorization from a non-affiliated customer to share its information with a Marketing Function Employee, the Transmission Provider will post a notice, on a NU Transmission Web page specifically created for these types of information sharing, of the customer consent accompanied with a statement that it did not provide any preferences, either operational or rate-related, in exchange for that voluntary consent.

This posting requirement is reflected in the FERC Order No. 717 website posting procedures maintained by employees of NU's transmission function.

* * * * *

(d) Posting written procedures on the public Internet. A transmission provider must post on its Internet website current written procedures implementing the standards of conduct.

Procedures and Mechanisms for Ensuring Compliance

The NU Compliance Plan was initially posted to the NU Transmission website in December 2008. Updates to the Plan have since been posted to reflect organizational and procedural modifications. The Plan is also posted on the NSTAR website found at http://www.nstar.com/business/rates_tariffs/open_access.

* * * * *

(e) Identification of affiliate information on the public Internet.

(1) A transmission provider must post on its Internet website the names and addresses of all its affiliates that employ or retain marketing function employees.

(2) A transmission provider must post on its Internet website a complete list of the employee-staffed facilities shared by any of the transmission provider's transmission

function employees and marketing function employees. The list must include the types of facilities shared and the addresses of the facilities.

Procedures and Mechanisms for Ensuring Compliance

The Web pages displaying all FERC Order No. 717 posting requirements are clearly displayed and accessible from the Transmission external website. The OASIS Web pages reside in the section entitled "Rates, Tariffs and Interconnections" on the Transmission home page (http://www.transmission-nu.com/ and http://www.nstar.com/business/rates_tariffs/open_access).

The following information is presented in these pages:

- The names and addresses of all its affiliates that employ or retain Marketing Function employees
- A complete list of the employee-staffed facilities shared by any of the transmission provider's transmission function employees and Marketing Function employees. The list includes the types of facilities shared and the addresses of the facilities.

Procedures are in place specifying the form and content of the affiliate information to be posted on the OASIS Web site. The forms necessary to post this information are available to authorized employees on the OASIS Web site maintained by NU transmission employees.

NU will update the Web site information within seven business days of any change, and post the date on which the information was updated.

* * * * *

(3) The transmission provider must post information concerning potential merger partners as affiliates that may employ or retain Marketing Function employees, within seven days after the potential merger is announced.

Procedures and Mechanisms for Ensuring Compliance

The posting procedures note that any NU Transmission Provider will post pertinent information related to any merger activities that affiliates may engage in. NU and NSTAR have specific pages established on their respective Transmission websites for notices required in this Section.

* * * * *

(f) Identification of employee information on the public Internet.

(1) A transmission provider must post on its Internet website the job titles and job descriptions of its transmission function employees.

Procedures and Mechanisms for Ensuring Compliance

The posting procedures note that any NU Transmission Provider will post the job titles and job descriptions of its transmission function employees. NU has a specific page established on its Transmission Web site for notices required in this Section.

* * * * *

(2) A transmission provider must post a notice on its Internet website of any transfer of a transmission function employee to a position as a marketing function employee, or any transfer of a marketing function employee to a position as a transmission function employee. The information posted under this section must remain on its Internet website for 90 days. No such job transfer may be used as a means to circumvent any provision of this part. The information to be posted must include:

(i) The name of the transferring employee,
(ii) The respective titles held while performing each function (i.e., as a transmission function employee and as a marketing function employee), and
(iii) The effective date of the transfer.

Procedures and Mechanisms for Ensuring Compliance

The OASIS Web site posting procedures explain that employee transfers must be posted, including the name of the transferring employee, the respective titles held while performing each function, and the effective transfer date. The employee transfer information must remain on the OASIS for 90 days.

Employee transfers are to be reported by the NUSCO Human Resources (HR) Staffing Unit to the Corporate Compliance Manager and the Transmission HR Manager. The HR Manager, in turn, is responsible for ensuring that any transfer is posted on both the NU and NSTAR websites.

* * * * *

(g) Timing and general requirements of postings on the public Internet.

(1) A transmission provider must update on its Internet website the information required by this part 358 within seven business days of any change, and post the date on which the information was updated. A public utility may also post the information required to be posted under part 358 on its OASIS, but is not required to do so.

Procedures and Mechanisms for Ensuring Compliance

Transmission function employees will update the website information within seven business days of any change, and post the date on which the information was updated.

* * * * *

(2) In the event an emergency, such as an earthquake, flood, fire or hurricane, severely disrupts a transmission provider's normal business operations, the posting requirements in this part may be suspended by the transmission provider. If the disruption lasts longer than one month, the transmission provider must so notify the Commission and may seek a further exemption from the posting requirements.

Procedures and Mechanisms for Ensuring Compliance

The OASIS posting procedures administered in the Transmission Group note that posting requirements may be suspended by Transmission Group management in the event of a disruption in normal business operations.

* * * * *

(3) All Internet website postings required by this part must be sufficiently prominent as to be readily accessible.

Procedures and Mechanisms for Ensuring Compliance

The Web pages displaying all FERC Order No. 717 posting requirements are clearly displayed and accessible from the Transmission external website. The OASIS Web pages reside in the section entitled "Rates, Tariffs and Interconnections" on the Transmission home page (http://www.transmission-nu.com/ and http://www.nstar.com/business/rates_tariffs/open_access).

* * * * *

(h) Exclusion for and recordation of certain information exchanges.

(1) Notwithstanding the requirements of §§ 358.5(a) and 358.6, a transmission provider's transmission function employees and marketing function employees may exchange certain non-public transmission function information, as delineated in § 358.7(h)(2), in which case the transmission provider must make and retain a contemporaneous record of all such exchanges except in emergency circumstances, in which case a record must be made of the exchange as soon as practicable after the fact. The transmission provider shall make the record available to the Commission upon request. The record may consist of hand-written or typed notes, electronic records such as e-mails and text messages,

recorded telephone exchanges, and the like, and must be retained for a period of five years.

(2) The non-public information subject to the exclusion in § 358.7(h)(1) is as follows:

(i) Information pertaining to compliance with Reliability Standards approved by the Commission, and

(ii) Information necessary to maintain or restore operation of the transmission system or generating units, or that may affect the dispatch of generating units.

Procedures and Mechanisms for Ensuring Compliance

The prohibition against transmission function employees from conducting marketing functions is explained in the EEI training module on FERC Order No. 717. The training materials note that a contemporaneous record must be kept for these types of information exchanges.

* * * * *

(i) Posting of waivers. A transmission provider must post on its Internet website notice of each waiver of a tariff provision that it grants in favor of an affiliate, unless such waiver has been approved by the Commission. The posting must be made within one business day of the act of a waiver. The transmission provider must also maintain a log of the acts of waiver, and must make it available to the Commission upon request. The records must be kept for a period of five years from the date of each act of waiver.

Procedures and Mechanisms for Ensuring Compliance

The OASIS posting procedures administered by NU's transmission function state that they must post waivers, if any, of a tariff provision that it grants in favor of an affiliate unless previously approved by the Commission. Further, the procedures note the one day posting requirement, the need to maintain a log of any waivers, and the need to make the log available to the Commission.

* * * * *

§ 358.8 Implementation requirements.

(a) Effective date.
A transmission provider must be in full compliance with the standards of conduct on the date it commences transmission transactions with an affiliate that engages in marketing functions.

Procedures and Mechanisms for Ensuring Compliance

NU Transmission Providers and affiliates were in full compliance with the Standards of Conduct by November 26, 2008. Further, NU's Compliance Plan for the Standards is posted to the OASIS Web site.

* * * * *

(b) Compliance measures and written procedures.

(1) A transmission provider must implement measures to ensure that the requirements of §§ 358.5 and 358.6 are observed by its employees and by the employees of its affiliates.

Procedures and Mechanisms for Ensuring Compliance

The detailed procedures and mechanisms documented in § 358.5 and § 358.6 (i.e., IT and physical separation), in addition to those related to other sections, were initially reflected in a comprehensive compliance plan posted to OASIS in December 2008. The Standards of Conduct training module referred to earlier also heightens employee awareness of the Order No. 717 requirements.

* * * * *

(2) A transmission provider must distribute the written procedures referred to in § 358.7(d) to all its transmission function employees, marketing function employees, officers, directors, supervisory employees, and any other employees likely to become privy to transmission function information.

Procedures and Mechanisms for Ensuring Compliance

The detailed procedures and mechanisms displayed in this Compliance Plan have been distributed to all Transmission Function employees and Marketing Function employees.

* * * * *

(c) Training and compliance personnel.

(1) A transmission provider must provide annual training on the standards of conduct to all the employees listed in paragraph (b)(2) of this section. The transmission provider must provide training on the standards of conduct to new employees in the categories listed in paragraph (b)(2) of this section, within the first 30 days of their employment. The transmission provider must require each employee who has taken the training to certify electronically or in writing that s/he has completed the training.

Procedures and Mechanisms for Ensuring Compliance

A comprehensive training program is the primary means for ensuring compliance with the various State and Federal codes of conduct at NU. Mandatory, department-specific training began in 1999 and continues to be used to educate employees throughout the NU System.

Transmission Function employees, Marketing Function employees, shared services, and certain distribution company employees have received training regarding FERC Order No. 717 rules and reporting requirements. Further, these employees will produce electronic certifications verifying that they have been trained, understand FERC Order No. 717 and will abide by its rules.

* * * * *

(2) A transmission provider must designate a chief compliance officer who will be responsible for standards of conduct compliance. The transmission provider must post the name of the chief compliance officer and provide his or her contact information on its Internet website.

Procedures and Mechanisms for Ensuring Compliance

NU management has designated Duncan R. MacKay, NU Deputy General Counsel and Chief Compliance Officer, as the FERC Chief Compliance Officer responsible for administering compliance with the Standards of Conduct. Mr. MacKay's contact information is posted on the NU and NSTAR internet websites.

* * * * *

(d) Books and records.

A transmission provider must maintain its books of account and records (as prescribed under parts 101, 125, 201 and 225 of this chapter) separately from those of its affiliates that employ or retain marketing function employees, and these must be available for Commission inspections.

Procedures and Mechanisms for Ensuring Compliance

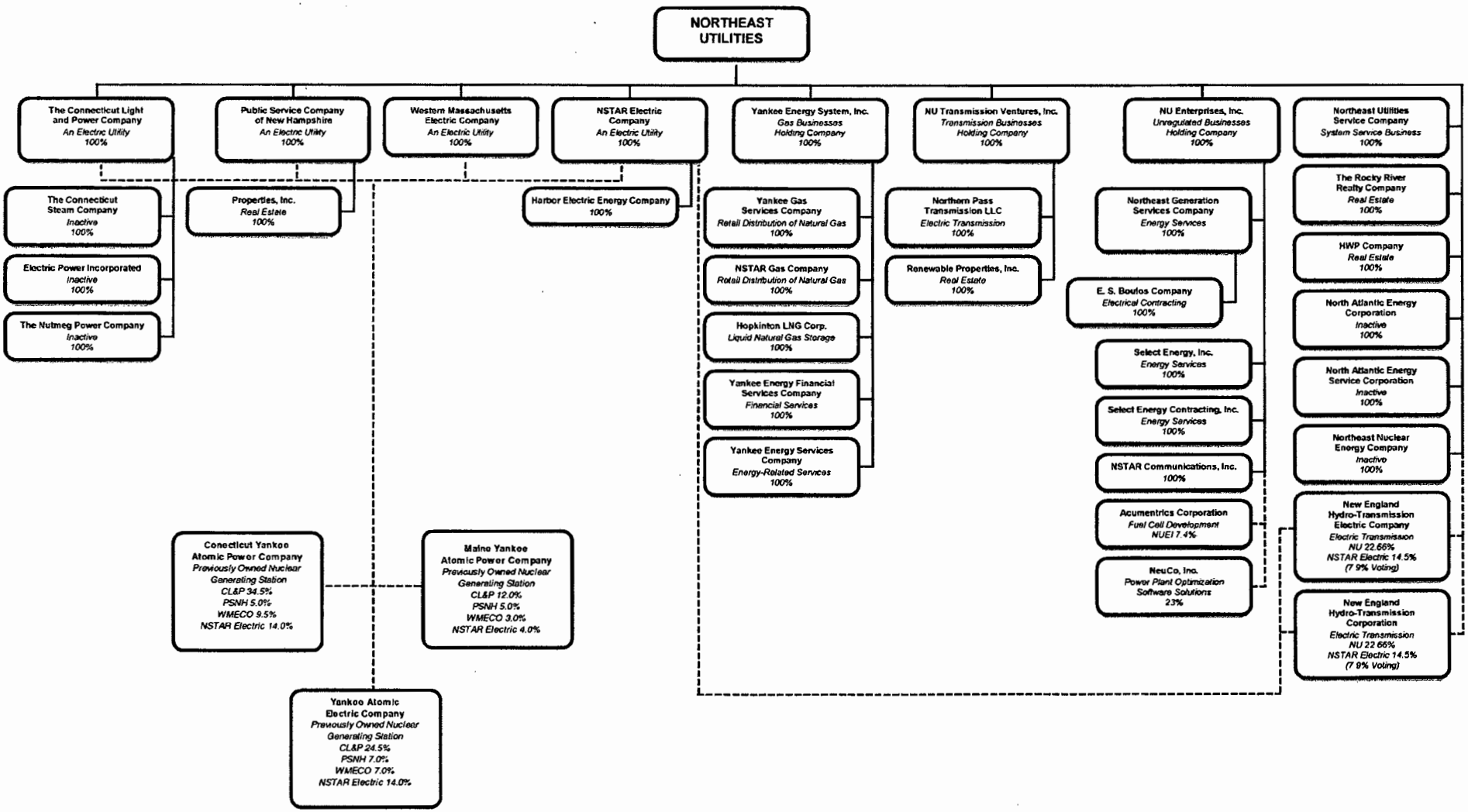
Each of the NU System Companies maintain separate books and records. NU subsidiaries follow and will continue to follow Uniform System of Accounts and Records (USOA) and Generally Accepted Accounting Principles (GAAP) standards, to the extent applicable. The books and records of NU's Transmission Providers and Marketing Function affiliates are open for examination by the Commission.

* * * * *

APPENDIX A

NORTHEAST UTILITIES SYSTEM CORPORATE CHART

EFFECTIVE MAY 30, 2014



NORTHEAST UTILITIES SUBSIDIARIES AND AFFILIATES

Northeast Utilities (NU) is the parent company of the NU system, one of the largest utility systems in the country and the largest in New England.

The Connecticut Light and Power Company (CL&P) is Connecticut's largest electric utility, serving approximately 1.2 million customers throughout the state of Connecticut.

The Connecticut Steam Company, Electric Power Incorporated, and The Nutmeg Power Company are inactive specially chartered companies.

Connecticut Yankee Atomic Power Company (CYAPC) owned a nuclear generating plant that has been decommissioned. CL&P owns 34.5% of CYAPC.

Yankee Atomic Electric Company (YAEC) owned a nuclear generating plant that has been decommissioned. CL&P owns 24.5% of YAEC.

Maine Yankee Atomic Power Company (MYAPC) owned a nuclear generating plant that has been decommissioned. CL&P owns 12% of MYAPC.

Public Service Company of New Hampshire (PSNH) is New Hampshire's largest electric utility serving about 500,000 customers throughout the state of New Hampshire.

Properties, Inc. owns non-utility real estate in New Hampshire.

CYAPC. PSNH owns 5% of CYAPC.

YAEC. PSNH owns 7% of YAEC.

MYAPC. PSNH owns 5% of MYAPC.

Western Massachusetts Electric Company (WMECO) is an electric utility serving more than 200,000 customers throughout the western portion of the Commonwealth of Massachusetts.

CYAPC. WMECO owns 9.5% of CYAPC.

YAEC. WMECO owns 7% of YAEC.

MYAPC. WMECO owns 3% of MYAPC.

NSTAR Electric Company (NSTAR Electric) is an electric utility serving more than 1.1 million customers in 81 cities and towns (including Boston) in the Commonwealth of Massachusetts.

Harbor Electric Energy Company provides retail distribution and other services to the Massachusetts Water Resources Authority.

CYAPC. NSTAR Electric owns 14% of CYAPC.

YAEC. NSTAR Electric owns 14% of YAEC.

MYAPC. NSTAR Electric owns 4% of MYAPC.

New England Hydro-Transmission Electric Company is an electric transmission company of which NSTAR Electric owns 14.5% (7.9% voting).

New England Hydro-Transmission Corporation is an electric transmission company of which NSTAR Electric owns 14.5% (7.9% voting).

Yankee Energy System, Inc. (YES) is the holding company for the following subsidiaries:

Yankee Gas Services Company is Connecticut's largest natural gas distribution company, serving approximately 208,000 customers in 71 cities and towns.

NSTAR Gas Company (NSTAR Gas) is a natural gas distribution company serving approximately 300,000 customers in 51 cities and towns in the Commonwealth of Massachusetts.

Hopkinton LNG Corp. owns and controls liquid natural gas storage facilities used by NSTAR Gas during the winter heating season.

Yankee Energy Financial Services Company (YEFSCO) provides energy equipment financing. YEFSCO is in the process of winding down its business.

Yankee Energy Services Company (YESCO) provided energy-related services. YESCO is in the process of winding down its business.

NU Transmission Ventures, Inc. is the holding company for Northern Pass Transmission LLC and Renewable Properties, Inc.

Northern Pass Transmission LLC will construct, own and operate The Northern Pass transmission project with Hydro Quebec.

Renewable Properties, Inc. was formed to own real estate in New Hampshire in connection with activities relating to The Northern Pass transmission project.

NU Enterprises, Inc. (NUEI) is the holding company for NU's competitive businesses.

Northeast Generation Services Company (NGS) has completed all of its contractual operating obligations. NGS provides operational and reporting oversight to E. S. Boulos Company.

E. S. Boulos Company provides electrical contracting services in New England.

Select Energy, Inc. (Select Energy) previously provided energy services and held wholesale competitive energy contracts, of which the last one expired at the end of 2013. Select Energy is in the process of being dissolved.

Select Energy Contracting, Inc. (SECI) was formerly engaged in HVAC and related work. SECI is in the process of being dissolved.

NSTAR Communications, Inc. installs, owns, operates and maintains data transport networks for other telecom service providers in Boston to deliver voice, data, and other services to customers.

Acumentrics Corporation is a fuel cell development company of which NUEI owns 7.4%.

NeuCo, Inc. is a provider of power plant optimization software solutions of which NUEI owns 23%.

Northeast Utilities Service Company provides centralized accounting, administrative, information resources, engineering, financial, legal, regulatory, operational, planning, purchasing and other professional services to NU and its subsidiaries.

The Rocky River Realty Company (RRR) owns and leases non-utility real estate in Connecticut and Massachusetts. NorConn Properties, Inc., formerly a subsidiary of YES, and The Quinnehtuk Company, formerly a direct subsidiary of NU, were merged into RRR on August 31, 2009.

HWP Company, formerly known as Holyoke Water Power Company, owns limited, non-utility real estate in Holyoke, Massachusetts.

North Atlantic Energy Corporation (NAEC) owned PSNH's share of the Seabrook nuclear generating facility (Seabrook) which was sold to FPL in 2002. NAEC is in the process of winding down its business.

North Atlantic Energy Service Corporation (NAESCO) was agent for the joint owners of Seabrook prior to its sale. NAESCO is in the process of winding down its business.

Northeast Nuclear Energy Company (NNECO) was agent for the joint owners of the Millstone nuclear generating facilities, which were sold to Dominion Resources in 2001. NNECO is in the process of winding down its business.

New England Hydro-Transmission Electric Company is an electric transmission company of which NU owns 22.66%.

New England Hydro-Transmission Corporation is an electric transmission company of which NU owns 22.66%.

APPENDIX B

Regulatory Code of Conduct: Affiliate Transaction Principles

Federal and state regulatory Codes of Conduct are in effect that regulate transactions between regulated and energy marketing affiliates.

Nondiscrimination

- The NU Operating Companies shall not give any preference of any kind to their energy marketing affiliates or customers of their energy marketing affiliates.

- The NU Operating Companies shall provide electric energy market participants nondiscriminatory access to their transmission and distribution facilities.

- In tariff administration, the NU Operating Companies shall strictly enforce tariff provisions where there is no provision for discretion in the tariff. To the extent a tariff provides for discretion, such provision shall be applied in the same manner to the NU Operating Companies energy marketing affiliates and their customers and all unaffiliated electric market participants and their customers.

- The NU Operating Companies shall process requests for similar services provided by the NU Operating Companies in the same manner and within the same time frame for their energy marketing affiliates and for unaffiliated electric market participants.

Pricing for Transfers of Goods, Services and Assets

To the extent that the regulatory Codes of Conduct do not prohibit transfers of goods and services between the NU Operating Companies and their energy marketing affiliates, such transfers shall be subject to the following pricing provisions:

- Transfers from any of the NU Operating Companies to any energy marketing affiliates of goods and services produced, purchased or developed for sale on the open market by any of all of the NU Operating Companies will be priced at fair market value.

- Transfers from energy marketing affiliates to any or all of the NU Operating Companies of goods and services produced, purchased or developed for sale on the open market by the energy marketing affiliate shall be priced at fair market value.

- Transfers from one or more NU Operating Company(ies) to another NU Operating(ies) shall be at fully loaded cost.

- Goods or services that are price regulated by a state or federal agency shall be transferred at the tariffed or regulated rate.

Pricing and Allocation for Joint Purchases or Shared Costs

Joint purchases or shared costs permitted under the Regulatory Codes of Conduct shall be allocated and priced to the NU Operating Companies and the energy marketing affiliates based on actual embedded costs or as otherwise determined by the state or federal regulatory agency having jurisdiction over the transaction.

Discounts

- If the NU Operating Companies offer a discount or fee waiver to any energy marketing affiliates, such discount shall be made available contemporaneously to all unaffiliated electric energy suppliers serving the same market.

- The NU Operating Companies shall not create a unique discount arrangement with any energy marketing affiliates so that no competitor could be considered as serving the same market.

- Discounts provided by CL&P to its energy marketing affiliates shall be posted on the Affiliate Discount Report located on the CL&P website as required by the Connecticut Code of Conduct.

Recordkeeping

- All transactions among the NU Operating Companies and their energy marketing affiliates (including contracts and related bids).

- The record of the transaction shall include at a minimum: (a) the name of the parties to the transaction, (b) a description of the transaction, (c) the time period over which the transaction will occur, and (d) the terms and conditions of the transaction.

- These records shall conform to all applicable state and federal requirements and shall be maintained for a minimum of three years or longer if required by a state or federal agency. These records shall also be available for review by state or federal agencies having jurisdiction over them pursuant to the applicable

state and federal regulatory requirements.

APPENDIX C

Affiliate Rules: Codes of Conduct for Regulated and Marketing Affiliates

Employees must comply with all applicable state or federal regulatory Codes of Conduct governing our industry when doing business with NU affiliates. At NU, our regulated Wholesale Power Supply group is considered a marketing affiliate for purposes of these rules. An employee who discloses, accesses, seeks to access, uses or exploits in any manner restricted information in violation of the Regulatory Codes of Conduct will be subject to disciplinary action up to and including discharge.

Do's and Don'ts for employees of the Regulated Affiliates:

Do...

- Treat all customers fairly, regardless of their energy supplier.
- Treat all energy service companies fairly regardless of their affiliation.
- Charge all similarly situated customers the same prices for your services, regardless of their energy supplier.
- Keep customer-specific information confidential; release it only to the customer or the customer's authorized representative or energy supplier with written authorization.
- Keep non-customer specific, non-public information (e.g., distribution company electricity purchases, etc.) confidential unless it is also made contemporaneously and easily available to other service providers.
- Adhere to transfer pricing and cost allocation rules.

Don't...

- Provide sales leads for NU's marketing affiliates.
- Use your position to direct customers to do business with your side business or to a business in which you have a financial interest.
- Share customer-specific information with our marketing affiliates, unless they are the authorized agent of the customer.
- Share non-customer specific, non-public information with our marketing affiliates, unless the information is made available to all potential competitors at the same time.

- Represent to anyone that our marketing affiliates will receive preferential treatment.
- Engage in any joint marketing activities with our marketing affiliates.
- Give preferential treatment to customers of our marketing affiliates.

Do's and Don'ts for Marketing Affiliate Employees:

Do...

- Use the regulated company name (e.g., CL&P, PSNH, WMECO, NSTAR Electric, Yankee Gasand NSTAR Gas) and explain the affiliation with the regulated company via a written disclaimer.
- Adhere to cost allocation rules.

Don't...

- Represent to anyone that our marketing affiliates' customers will receive preferential treatment from the marketing business based on their relationship with the regulated company.
- Represent that customers of marketing affiliates will receive more reliable power than customers of other energy suppliers.
- Attempt to engage in any joint marketing efforts with the regulated company.
- Attempt to extract customer-specific or non-public information from regulated company employees.

General

Information that is related to providing administrative and general services may be shared, as long as marketing employees do not obtain access to restricted information. Examples include but are not limited to payroll, benefits, personnel, auditing, general accounting, rate design, treasury services, shareholder services, financial reporting, financial planning and analysis, corporate security, regulatory affairs, lobbying, legal, IT and general purchasing.

NU has established separate shared areas on the Local Area Network (LAN) for regulated and marketing information. Information generated by or on behalf of the

regulated function must not be stored in or moved to any shared area, including NU's internal Web site (NUNet), unless it has been specifically established for the regulated function or appropriately secured.

Restricted information must not be input into any mainframe application unless such information is encrypted or an electronic security measure has been installed to protect the information.

NU's computer systems are subject to periodic audits to ensure these provisions comply with the Regulatory Codes of Conduct.

Certain Codes of Conduct restrict movement of employees between regulated and marketing affiliates, or between transmission and marketing affiliates. For purposes of the Federal Standards of Conduct, the Corporate Compliance Manager must be informed in order to post certain employee transfers to the appropriate Transmission website. Additional information is provided in "Codes of Conduct Employee Transfer Procedures."

Contact Information:

Scott Devendorf
Corporate Compliance Manager
Legal Department, Berlin BME-2
Office: 860-665-2004
E-mail Address: scott.devendorf@nu.com

Phyllis Lemell
Assistant General Counsel
Legal Department, Berlin BME-2
Office: 860-665-5118
E-mail Address: phyllis.lemell@nu.com

APPENDIX D

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

Home | Marketing Function Employees | Transmission Providers | Compliance Contact | Glossary | Next

Generic | slide 1 of 26 in this section

INTRODUCTION

Welcome to the Edison Electric Institute (EEI) Training Program on FERC's Standards of Conduct. EEI is the association of the nation's shareholder-owned utilities and their affiliates worldwide.

This program was developed by EEI in conjunction with the law firm of Skadden, Arps, Slate, Meagher & Flom LLP. In assisting EEI in the development of this program, Skadden Arps was providing advice solely to EEI. Skadden Arps was not providing advice to, or representing, EEI member companies or others who may purchase this product from EEI.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

INSTRUCTIONS

Once you have read and understood the material on a page, click the "next" button at the top of the page. If a term is not familiar to you, you can click the "Glossary" link at the top of the page. Additionally, you can click on highlighted words to see their definitions. At the end you will be asked to answer "quiz" questions, and you will receive feedback explaining why your answer to each question was right or wrong.

EDISON ELECTRIC INSTITUTE

Leadership in partnership with electricity users

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

Home | Marketing Function Employees | Transmission Providers | Compliance Contact | Glossary

◀ Back | Next ▶

Generic | slide **3** of **26** in this section

THE RULES (AND THE TRAINING) HAVE CHANGED

If you haven't taken the EEI Standards of Conduct training for a couple of years, you will notice that it has been substantially revised. This is because the rules have changed. The rules have been simplified and clarified to better achieve FERC's goals of compliance and enforcement. The rules now apply more based on what an employee does, and less based upon the company affiliate or business unit that the employee works for. Among other things, this has resulted in changes to the definitions of "marketing functions" and "transmission functions," and elimination of the concept of "Energy Affiliates."

The rules also have taken somewhat different approaches to application to electric and gas transmission providers. This training focuses on electric transmission providers. For questions about application of the rules to gas pipeline transmission providers, contact your compliance contact.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

100% COMPLIANCE IS EXPECTED AT NU

You must understand and adhere to the Standards of Conduct.

The Federal Energy Regulatory Commission ("FERC") can impose substantial penalties or other remedies for violations of the Standards of Conduct. These include loss of our market-based rates and fines of *millions of dollars*.

Compliance is part of your job!

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

PURPOSE OF TRAINING

The goal of this training is to ensure two things:

(1) a solid understanding of how the rules apply to you *and* (2) an understanding of when to ask for help

There is no shame in asking for help interpreting the rules - to the contrary, it is expected and required.

So the most important lesson is this: when in doubt, ask.

Click here for contact information regarding compliance questions. You can also click on the compliance contact link above, which appears on every page of the training.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

CORE PRINCIPLES OF THE STANDARDS OF CONDUCT

The core principles behind the Standards of Conduct are that a transmission provider must treat **ALL** transmission customers, affiliated and non-affiliated, on a non-discriminatory basis, and cannot operate its transmission system to give a preference to its marketing function, marketing function employees, or to an affiliate, or to any person in matters relating to the sale of transmission service. In particular, affiliated transmission customers should not be given preferential transmission service or preferential access to information about the transmission system.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

THE KEY TO UNDERSTANDING THE RULES IS KNOWING WHERE THE WALL IS

The Standards of Conduct generally impose restrictions on interactions between:

(a) the employees of the transmission provider who operate the transmission system on a day-to-day basis (transmission function employees),

and

(b) the employees of the transmission provider and affiliates who engage on a day-to-day basis in power marketing (marketing function employees).

However, through the "no-conduit rule" the Standards of Conduct affect all employees of NU. The key to understanding the Standards of Conduct is understanding how it affects your relationship with other employees of NU.; IF YOU ARE NOT SURE OF YOUR CLASSIFICATION UNDER THE STANDARDS OF CONDUCT, ASK YOUR COMPLIANCE CONTACT.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

Home | Marketing Function Employees | Transmission Providers | Compliance Contact | Glossary

◄ Back | Next ►

Generic | slide 8 of 26 in this section

THE KEY TO UNDERSTANDING THE RULES IS KNOWING WHERE THE WALL IS

The two sets of employees might be thought of as being on opposite sides of a Wall. On one side of the Wall are "transmission function employees." Transmission function employees may include people who are not directly employed by the transmission provider, such as agents, contractors or consultants.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

WHO IS A TRANSMISSION FUNCTION EMPLOYEE?

A person is a transmission function employee if he/she actively and personally engages in the day to day operation of the transmission system. This includes planning, directing, organizing or carrying out the following activities:

Granting or denying requests for transmission (including requests for ancillary services under the OATT and requests for interconnection).

Coordinating actual physical flows of power.

Isolating portions of the system to prevent cascades.

Imposing transmission loading relief.

Other similar activities.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

Home | Marketing Function Employees | Transmission Providers | Compliance Contact | Glossary

Back | Next

Generic | slide 10 of 26 in this section

WHO IS NOT A TRANSMISSION FUNCTION EMPLOYEE?

The following employees are generally not considered transmission function employees if functioning in their stated capacity: field, maintenance and construction workers, engineers, clerks, attorneys, accountants, risk management personnel, regulatory personnel, rate design personnel, strategic planning personnel, and long range transmission planners.

However, a title is not a shield against being a transmission function employee. Someone who meets the criteria for a transmission function employee *is* a transmission function employee, regardless of whether the employee also fits one of the categories above.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

WHO IS A MARKETING FUNCTION EMPLOYEE?

On the other side of the Wall is another group of people called marketing function employees.

Generally, marketing function employees are employees of the transmission provider or its affiliates who engage on a day-to-day basis in marketing functions. Marketing functions include selling power at wholesale, selling ancillary services at market-based rates, reselling physical or financial transmission rights, or make offers of energy capacity, demand response, or other products into an organized market run by an RTO or ISO.

An employee is a marketing function employee if he or she performs any marketing function, even if some of his or her other activities (e.g., purchases of power) are not marketing functions.

The following are not marketing functions:

> Bundled retail sales – which FERC defines to include provider of last resort ("POLR") sales. However, other retail sales (sometimes referred to as competitive retail sales) are marketing functions.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

WHO IS NOT A MARKETING FUNCTION EMPLOYEE?

The following employees are generally not considered marketing function employees unless they engage in marketing functions: generation operators, analysts, forecasters, field, maintenance and construction workers, engineers, clerks, attorneys, accountants, risk management personnel, regulatory personnel, rate design personnel, and strategic planning personnel.

However, a title is not a shield against being a marketing function employee. Someone who meets the criteria for a marketing function employee is a marketing function employee, regardless of whether the employee also fits one of the categories above.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

SEPARATION OF FUNCTIONS

Transmission function employees must operate separately from marketing function employees. This means:

Transmission function employees cannot perform marketing functions (such as selling power at wholesale).

Marketing function employees cannot perform transmission functions (such as day-to-day operation of the transmission system).

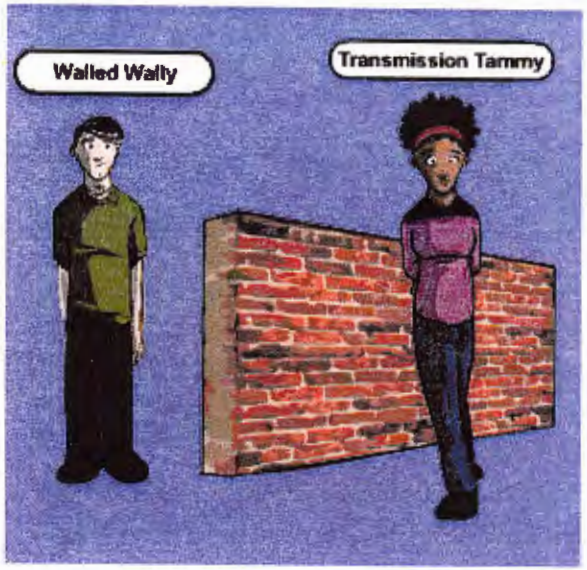
Marketing function employees cannot have access to the control room or other sensitive areas except on the same basis as the company provides access to other, non-affiliated transmission customers.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

SEPARATION OF TRANSMISSION FUNCTION AND MARKETING FUNCTION EMPLOYEES



Meet Transmission Tammy and Walled Wally. Tammy is a transmission function employee, and Wally is a marketing function employee.

In order to meet the independent functioning requirement, Transmission Tammy is restricted to the transmission side of the wall. She can't sell power because that would make her a marketing function employee.

Conversely, Walled Wally is restricted to the other side of the wall. He can't operate the transmission system, because he can't perform transmission functions.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

Home | Marketing Function Employees | Transmission Providers | Compliance Contact | Glossary

Back | Next

Generic | slide 15 of 26 in this section

SEPARATION OF FUNCTIONS - INDEPENDENT FUNCTIONING REQUIREMENT FOR SUPERVISORS

Meet VP Val. Both Transmission Tammy and Walled Wally report to VP Val. VP Val needs to be able to supervise both of their departments, but she also needs to recognize the wall that divides them. In order to have this responsibility, VP Val cannot actively and personally engage in transmission functions or marketing functions.

For example, she cannot participate in day-to-day transmission systems operations (which is a transmission function). She also cannot negotiate wholesale power sales agreements (which is a marketing function). If VP Val performs these functions for one side, she can no longer have responsibility for the other.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

SEPARATION OF FUNCTIONS - INDEPENDENT FUNCTIONING REQUIREMENT FOR OTHER EMPLOYEES

No-Conduit Ned is in a similar situation to VP Val. He could be a support employee, like a lawyer or accountant, or a field employee like a lineman, or a maintenance employee maintaining generation and/or transmission. The wall does not stop Ned from performing his function for either Transmission Tammy or Walled Wally, but like VP Val, he can't have that shared role if he performs transmission functions or marketing functions.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

INFORMATION SHARING RESTRICTIONS

Restrictions on sharing of transmission information called the "no-conduit" rule lie at the heart of the Standards of Conduct, and are the rules most frequently put to use day-to-day.
With a few narrow exceptions, transmission function employees are prohibited from sharing non-public transmission function information with marketing function employees other than through the Internet Website (which can be OASIS). So are other people at your company. Note, however, that this restriction only applies to *non-public* transmission function information.

If a marketing function employee improperly receives non-public transmission function information, the information may need to be posted *immediately* on the Internet Website.

If you believe that non-public transmission function information that is *not* posted on the Internet Website has been disclosed to a marketing function employee, and may not meet an exception, you must contact the compliance contact immediately.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

Home | Marketing Function Employees | Transmission Providers | Compliance Contact | Glossary

◀ Back | Next ▶

Generic | slide 18 of 26 in this section

INFORMATION SHARING RESTRICTIONS

Transmission function information is information that relates to transmission functions. Transmission function information includes information about available transmission capacity (or similar measurements), outages, the price of transmission (including interconnection and OATT ancillary services), curtailments and balancing, and similar types of information. It also includes information about granting or denying transmission service requests, including any information provided by an actual or potential transmission customer in the course of requesting service.

Determining whether information is non-public transmission function information is often case-specific and complicated. An improper classification can create significant risk. If you have any doubt, contact the Compliance Contact before non-public information is given to a marketing function employee. Information that may be non-public transmission function information should never be given to someone unless everyone involved is sure the person receiving the information is not a marketing function employee.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

Home | Marketing Function Employees | Transmission Providers | Compliance Contact | Glossary

Back | Next

Generic | slide 19 of 26 in this section

INFORMATION SHARING RESTRICTIONS - LIMITED EXCEPTIONS

There are some very limited exceptions to the prohibition on disclosure of non-public transmission function information to marketing function employees other than on the company's Internet Website. No one should use an exception to communicate non-public transmission function information to a marketing function employee without asking the Compliance Contact or the appropriate supervisor if it is ok. In general terms, the exceptions are as follows:

Transmission function employees may discuss with marketing function employees the latter's specific request for transmission service (but not non-public matters beyond the specific request, such as outages or other system conditions).

A transmission customer may voluntarily consent, in writing, to allow the transmission provider to disclose the transmission customer's non-public information to the transmission provider's marketing function employees. The transmission provider must post notice on its Internet website of that consent, along with a statement that it did not provide any preferences, either operational or rate-related, in exchange for that voluntary consent.

A transmission provider may provide marketing function employees with non-public information pertaining to compliance with Reliability Standards approved by FERC but must make and retain records of any such exchange at the time of the exchange (though in an emergency, the record may be made later).

A transmission provider may provide marketing function employees with non-public information necessary to maintain or restore operation of the transmission system or generating units, or that

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

INFORMATION SHARING RESTRICTIONS - MEASURES

Because transmission providers can face punishment for disclosure of information, they take steps to prevent the *accidental* sharing of non-public transmission function information, and to make it more difficult for a single "rogue" marketing function employee to circumvent the rules. These steps usually include measures to ensure separation of physical workspaces as well as of computer systems and data. Marketing employees are not permitted to have preferential access to the system control center or similar facilities.

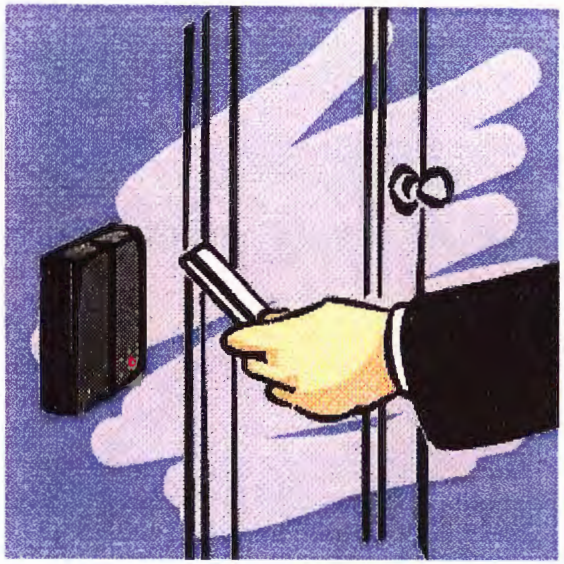
EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

INFORMATION SHARING RESTRICTIONS - MEASURES



Workspaces of transmission function employees usually are protected by features intended to prevent accidental disclosure of non-public transmission function information.

One example is card-key access that cannot be opened by marketing function employees, particularly in the transmission control center.

Another example is locks on filing cabinets or file rooms containing non-public transmission function information.

Be careful - these requirements are easy to overlook if workspaces are changed.

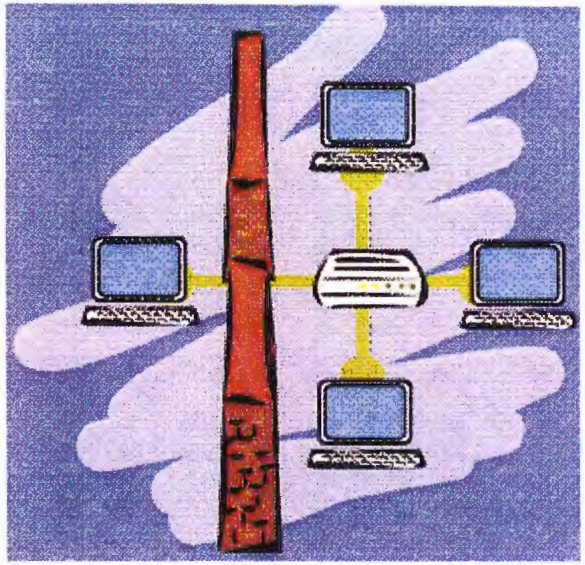
EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

INFORMATION SHARING RESTRICTIONS - MEASURES



Computer Networks usually have measures, such as password protection, firewalls or separate servers, to ensure that marketing function employees cannot access non-public transmission function information stored on the network.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

INFORMATION SHARING RESTRICTIONS - TRANSMISSION FUNCTION AND MARKETING FUNCTION EMPLOYEES

Transmission Tammy can't share non-public transmission function information with Walled Wally.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

Home | Marketing Function Employees | Transmission Providers | Compliance Contact | Glossary

Back | Next

Generic | slide 24 of 26 in this section

SEPARATION OF FUNCTIONS AND RESTRICTIONS ON INFORMATION SHARING: PUTTING IT TOGETHER

Because VP Val does not perform transmission or marketing functions, she can talk to both Tammy and Wally. The trick for her is making sure that when she learns non-public transmission function information from Tammy, she does not act as a ***conduit*** to pass the information on to Wally.

EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

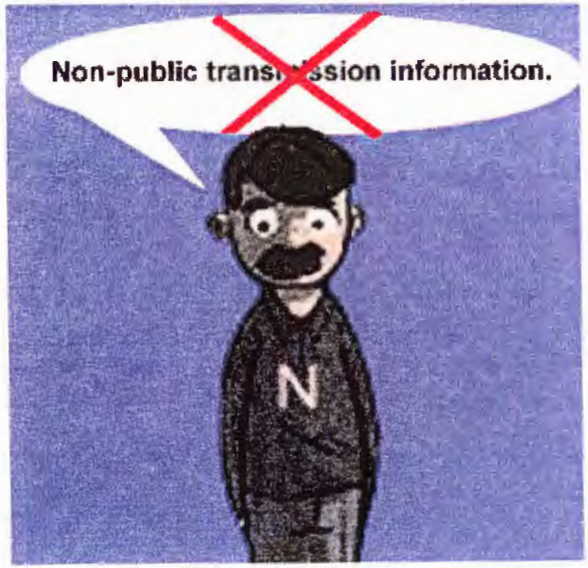
Instructions | Exit Course

Home | Marketing Function Employees | Transmission Providers | Compliance Contact | Glossary

◀ Back | Next ▶

Generic | slide 25 of 26 in this section

INFORMATION SHARING RESTRICTIONS - OTHER EMPLOYEES



No-Conduit Ned could be any employee or officer who is neither a transmission function employee nor a marketing function employee. He is still bound by the no-conduit rule. The rule may not apply much to Ned, because Ned may not come across much non-public transmission function information, but he needs to know it and follow it when it applies.

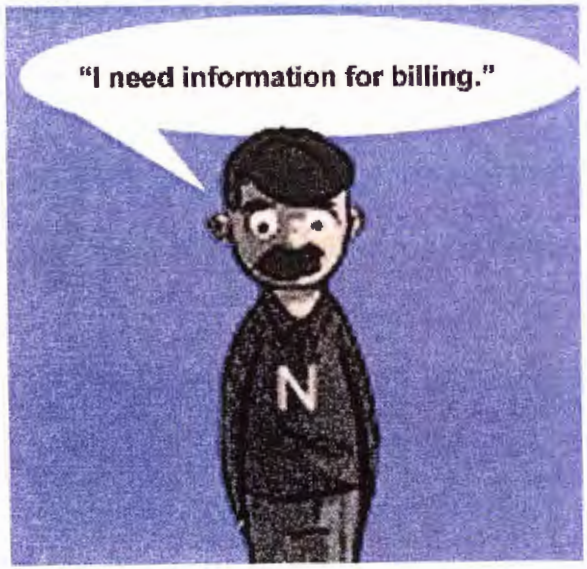
EDISON ELECTRIC INSTITUTE

Northeast Utilities System

EEI Training: Standards of Conduct

Instructions | Exit Course

SEPARATION OF FUNCTIONS AND RESTRICTIONS ON INFORMATION SHARING: PUTTING IT TOGETHER



The Standards of Conduct do not prevent No-Conduit Ned from talking to Walled Wally about things other than transmission function information. For instance, he may need to get customer load information from Wally in order to prepare bills for customers. However, he can't tell Wally about non-public transmission function information he obtains from Tammy in preparing the transmission bills.

APPENDIX E

Corporate Information Security ("CIS") Department

CIS uses a set of automated and manual tools and processes to enforce, monitor and administer access to the computers and information systems. NU's information security program is comprised of: 1) information security administration, and 2) electronic security. These components are described below.

1. Information Security Administration

CIS is responsible for protecting the computer and information systems from unauthorized access by managing and monitoring the computer and information security administration process. This group is responsible for enforcing both company security policies and applicable regulatory rules. These policies and rules are enforced by using Human Resources employee data, computer security software, and security administration procedures governing user access requests and approvals. This team of highly trained professionals is solely dedicated to enforcing the highest levels of computer and information security and separation.

NU's Internal Audit Department is responsible for ensuring that there are procedures in place for monitoring and insuring strict adherence to computer and information systems security standards. The audits review for compliance with

affiliate separation and access rules, and periodically test to ensure that employees of unregulated companies cannot access unauthorized utility computers, information systems, or data.

2. Electronic Security Systems and Procedures

A number of security mechanisms and processes are used to ensure that access to the regulated utility information systems and data is limited to authorized employees and functions. Employees assigned to an unregulated company cannot access computer applications supporting regulated utility business functions and containing data relating to the regulated utility. The following security systems and procedures, under the auspices of CIS, prevent unauthorized electronic access to, or the sharing of computers, information systems, or computer applications among affiliates and regulated utilities at both the data center and within distributed systems:

http://nunet.nu.com/Policies/NUPDetail.aspx?nup=34&category= Company Resources=

http://nunet.nu.com/T2AllPurpose.aspx?id=4294968324

The first document, the NU policy, gives CIS the authority to perform its responsibilities. The second document. the Corporate Information Security Procedure, identifies information owners and requires the establishment of an information classification program. This framework, which includes clear definitions for Confidential Information and assigned ownership's

(http://nunet.nu.com/T2AllPurpose.aspx?id=4294968629), significantly contributes to ensuring information access policy compliance.

Individual Employee Identifications and Passwords: Industry standard security software is used to read individual employee log-on identifications and passwords to approve or deny access to the computers, the applications running on the computers and the specific data stored and processed by the applications. The identifications and passwords are verified by the computer security system and also by the application that the employee is accessing. The administrators of the security system and the business owners of the applications maintain tables of user identifications and passwords that are checked by the computer systems to allow or deny access.

Basic Access Rule is to Deny Access by Default: The basic security policy for all Northeast Utilities computers and information systems is to deny access by default. This means that access is granted only when an employee provides the system with a valid Logon ID and password that has previously been issued after completion of an established approval process and the proper system validation lists have been updated.

Identification and Password Controls and Administration: The mainframe data center computer systems control access by processing Logon ID, password

and access rules that determine if access will be granted or denied and, if granted, what computer processes and data the user will be allowed to access.

Application Security: Application systems, such as time keeping, also use Logon ID and password to control access to the application, data, and functions within the application. Local application security administrators, designated by the business owner of the system or application, have the ability to grant, deny or remove access to the application itself, and to limit access to specific data and functions based on company policy and Regulatory Code of Conduct regulations.

Security Software: The mainframe computer resources within the data center use industry standard security software supplied by Computer Associates International Inc. This software is rated as Class C2, as defined by the National Security Agency in accordance with the Department of Defense's Trusted Computer System Evaluation Criteria. Security software rated in this category are typically used by large commercial and industrial customers in a variety of competitive industries. This software allows Northeast Utilities to isolate data center computer and information systems and data resources so that they cannot be accessed without proper authority.

Security Handling of Terminated and Transferred Employees: As terminations and transfers between regulated and unregulated companies occur, NU's Human Resources Department provides reports to Corporate Information

Security, who in turn will notify Business Unit application owners and security administrators, Information Technology Client Service Representatives, server administrators and other key personnel, as appropriate. These reports are used to remove access for the terminated and transferred employees.

The person transferring to an unregulated company will be responsible for ensuring that they not retain access to confidential or inappropriate data. This will include a signed statement stating that they have reviewed their data files and do not possess confidential information and that if at anytime they receive any, they will delete it and contact the sender to eliminate any future transmissions.

No data files on any computer platforms will be retained by the transferred employee unless reviewed and approved by the supervisor of the area from which they are transferring. The processes for handling each of the information technology platforms are outlined below:

E-Mail and Groupware (Lotus Notes): The owner of the account will be responsible to remove any documents and e-mails that contain confidential or inappropriate information, and notifying owners of mailing groups and Access Control Lists that they should be removed. Access to restricted Lotus Notes databases will be removed.

Mainframe: CIS will verify that transferring personnel have access to only those applications identified as appropriate for employees in an unregulated affiliate. CIS will also change their file accesses by changing their logon security record (ACF2) to the new functional area. The individual's originating supervisor in the regulated utility will review any existing datasets and determine which, if any, can be retained by the transferring employee. All others will be deleted or transferred to a person designated by the originating supervisor.

Business Unit Applications: In the event that the employee is retaining their personal computer, the IT Client Service Representative will be responsible for re-imaging the PC to remove access to all business unit-specific applications.

APPENDIX F

Home > Corporate > Departments

Corporate Information Security Procedure

1.0 Overview

This procedure provides specific instructions for implementing Northeast Utilities' (the Company's) Standards for Business Conduct regarding the Use of Technology and Confidential Information.

1.1 Purpose

Information in any form, including printed materials or electronic data, is an important asset of Northeast Utilities (the Company). The loss, corruption, and/or misuse of Company information

can adversely affect the Company's operations, financial condition and reputation, as well as the interests of the Company's employees, customers and/or investors. The protection of Company information is a basic employee responsibility. Employees should consult with their management as appropriate to assure that information is protected in a manner commensurate with its sensitivity, value, and criticality, each of which may change over time. This procedure is not intended to interfere with an individual's rights pertaining to safety concerns.

This procedure provides corporate level direction for the protection of all information and information technology assets regardless of the media on which the information is stored, the systems which process it or the methods by which it is moved. While laying the cornerstone for the Company's information security architecture, this procedure reinforces existing Company policies and standards.

1.2 Approach

As described in the Company's NUP 34: Confidential Information, it is the policy of the Company to protect the reliability and availability of information and the security and integrity of information technology systems. This procedure shall be implemented based on a philosophy of sharing information internal to the organization. Access to certain information will be appropriately restricted based on an identifiable need to protect the information. The Company shall develop, implement, and maintain cost-effective security measures to provide authorized access to information and to prevent unauthorized access to information.

1.3 Scope

The scope and applicability of this procedure are as follows:

- applies to all employees of the Company and its subsidiaries, as well as vendors, contractors, and agents developing and/or using Company information assets;
- applies independently of the way information is represented (e.g., written, spoken, electronic, etc.);
- applies independently of the technology used to handle the information (e.g., file cabinets, FAX machines, computers, answering machines, cellular telephone systems, local area networks, etc.);
- applies independently of the location of information (e.g., in an office, at a customer site, on an airplane, in an employee's home, etc.); and
- protects information throughout its life cycle (e.g., origination, entry into a system, processing, dissemination, storage, disposal, etc.).

2.0 Responsibilities

The primary responsibility for protecting the information technology and information assets of the Northeast Utilities system lies with every employee. Management has special responsibilities for implementing all administrative policies and procedures for information security, regardless of where the information is stored in a mainframe computer, a personal computer, a desk, a file cabinet or a waste basket. Management must ensure that all employees, vendors, and contractors are informed of their obligation to protect Company information assets.

2.1 User Responsibilities

Responsibility for information security rests with all employees, vendors, consultants, and contractors, on an on-going basis. The originator and all those with authorized access are responsible for the safekeeping of Company information in their custody. The user must use information and information technology assets only for the purpose intended and comply with established controls. User responsibilities include adhering to the following:

2.1.1 Password Procedures

2.1.2 Physical Security Procedures

2.1.3 Exchanging Information with Third Parties Procedures

2.1.4 Virus Protection Procedures

2.1.1. Password Procedures

Protect your passwords. Passwords are the user's key to Company computer systems. Passwords help to ensure that only authorized individuals access Company computer systems.

- Use strong passwords. Refer to Password Requirements for more details.
- DO NOT share your passwords.
- DO NOT store passwords in a data file, automatic log-in scripts, etc., unless access to this file is properly restricted.
- DO NOT post your password.
- **Password Compromise**. All passwords must be promptly changed if they are suspected of being disclosed or known to have been disclosed to unauthorized parties. Such incidents must be reported promptly to Corporate Information Security to determine if an investigation of unauthorized use is warranted.

Password Requirements
All passwords for your Company computer IDs must adhere to the following criteria. A strong password is relatively easy to remember but hard for others to guess and:

- must be 6 to 8 characters;
- must have at least one number;
- should be alphanumeric (a mix of letters and numbers);
- may contain one or more of the following symbols: @ # $
- must NOT contain any other special characters; and
- must NOT contain your User Name.

All passwords for CIP systems must adhere to the following criteria. A strong password is relatively easy to remember but hard for others to guess and:

- must be at least 8 characters;
- must be alphanumeric (a mix of letters and numbers); and
- must contain a symbol or special character*.

*For CIP systems, "symbols" or "special characters" are defined to include the following characters: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

There are a variety of techniques you can use to choose strong, secure passwords:

- Avoid passwords with any personal associations, e.g., family name, pet names, etc.
- Use non-words or easy-to-remember combinations of letters and numbers of six to eight characters.
- Use a word with digits embedded in it such as Tom87ato, Mon96day, or thr333ee.
- Use an acronym based on a nursery rhyme, a favorite song, movie, or sentence such as:
  - 3bmshtr - three blind mice, see how they run
  - atwin80d - Around the World in Eighty Days
- Drop vowels or drop everything but the first 6 letters of a long word and add digits or punctuation marks, such as:
  - mhs1swht - my house is white

- teleph0# - telephone numbers

- Choose a pattern that has unique personal meaning such as:
  - uni1ver - university
  - surpar30 - surprise party

Weak passwords are not acceptable for any Company computer ID. Weak passwords are easily guessed and include:

- any word that is found in the dictionary (of any language);
- the name of the user's significant other, friend or pet;
- telephone numbers;
- the user's license plate number;
- anything that can easily be tied to you personally, such as child name, pet name, birth date; and
- a string with the same characters, such as aaaaaa or 111111.

2.1.2. Physical Security Procedures

Reporting Lost or Stolen Identification Badges and System Access Tokens - Identification badges and physical access cards that have been lost or stolen-or are suspected of being lost or stolen-should be reported to the Corporate Security Department immediately. Likewise, all computer or communications system access tokens (e.g., smart cards with dynamic passwords, telephone credit cards, etc.) that have been lost or stolen-or are suspected of having been lost or stolen-should be reported to the Corporate Security Department immediately.

Reporting Stolen Information - If information is missing, contact your supervision, the information owner, and the Corporate Security Department.

Prevent unauthorized access to company technology.

- Ensure that the workstation screen lock is enabled when leaving a work area for an extended period of time.
- Log off your desktop computer by using the "Restart" option. At the end of each day or during extended absences, click on Start, Shutdown and choose the "Restart" option. Do not use the "Shut down" or "Log Off" options. **This does not apply to laptops, unless you have a secure locked office.** This process will enable various virus and software upgrades to be done during the evenings and thus create less impact on employees and network traffic.
- Maintain physical control of Company technology, including portable devices such as laptops, pagers, cell phones, PDAs, etc.
- During non-business hours, ensure that equipment is safe from unauthorized access or theft.
- It is recommended that users carry their equipment home with them when not at work. Should they choose to leave it at an NU Office, they should ensure that it is locked in a desk or office.
- Confidential information should never be stored on a laptop local (C:) drive unless the laptop is encrypted. Users with a business need to periodically, temporarily store confidential information on their laptop should contact Corp Info Security to confirm the laptop is encrypted.

2.1.3. Exchanging Information with Third Parties Procedures

All Company information must be protected from unauthorized disclosure. Refer to Information Security Requirements for details on how to determine the appropriate classification of Company information as Confidential, Internal Use, or Public.

1. **Lotus Notes Email** - transmission of email over the Internet is text-based (or "clear" text) and could be obtained by a third party.
   - Appropriate for Internal Use or Public information
   - Benefits and considerations of this option
   - For more information on using Notes email, submit an ITSC Electronic Ticket by logging on to any working computer or asking a co-worker to submit it on your behalf, and an analyst will respond in 2 hours or less.

2. **File Transfer Protocol (FTP)**- transmission of data over the Internet is text- based (or "clear" text) and could be obtained by a third party. Although the information in transit is not secure, the temporary storage area from where the file is to be retrieved is protected.
   - Appropriate for Internal Use or Public information
   - Benefits and considerations of this option
   - For NU client that require frequent large file exchanges over a long period of time (i.e., six months or longer) with only one or two third parties, an account on the FTP Server needs to be requested by following these steps:
     1. Complete the FTP Questionnaire
     2. Attach and send the questionnaire to Corp Info Security
     3. CIS will review, approve, and setup the account

   To maintain a copy for our records and for auditing purposes, the FTP Questionnaire information must be completed. Once reviewed and approved by CIS, an account (ID and Password) will be set up within 5 business days.
   The client is responsible for the account and can share the account with another client either inside or outside of NU to transfer data successfully to and from the FTP Server For NU clients who infrequently exchange large files and with various external parties, follow the FTP instructions. The third party will need to install some code on their PC to be able to retrieve files from a protected area on NU's FTP Server. Following this procedure eliminates the need for the client to request and manage a specific FTP account.
   For more information on these options, submit an ITSC Electronic Ticket by logging on to any working computer or asking a co-worker to submit it on your behalf, and an analyst will respond in 2 hours or less.

3. **Exchanging password protected WinZip files** - data is compressed or "zipped" then password protected before transmission, then password challenged and "unzipped" by the recipient upon a successful transmission. This method provides an improved level of protection since using a password encrypts the file and protects it from the casual eavesdropper. This option may be used with e- mail or FTP.
   - Appropriate for Internal Use or Public information, and for some Confidential information.
   - Benefits and considerations of this option
   - To launch WinZip on NU PCs, go to NU Programs, Accessories and select WinZip. The main WinZip window lists password protected files with a plus (+) sign following the filename. Here is some additional information you need to be aware of when using WinZip:

1. Using password security while using the Extract, CheckOut or Install Features: If you use the Extract, Test, CheckOut, or Install features on a password protected archive, you will automatically be prompted for the password.
2. To password protect files, it is important to specify the password AFTER opening or creating an archive and BEFORE adding the files. To password protect files in an archive:
    1. Open or create an archive. If you are using the New dialog box, uncheck the Add Dialog checkbox at the right of the dialog box.
    2. In the Add or Drop dialog box, click the Password button in the lower right hand corner of the window, and type a password.

This process can be shortened simply by following these steps:

1. Use Windows Explorer to find file you want to Zip.
2. Right click on the file and select Add to Zip option.
3. Click on the Password button in the lower right hand corner of the window.

After you create a password protected and "zipped" version of the file you want to send, follow the normal steps used for attaching a file to an email in Notes or use the FTP process described in Option 2 above. Remember, this password must be communicated via another medium (i.e., a telephone call) and should **not** be included in the email that contains the "zipped" file.

For more information on this option, submit an ITSC Electronic Ticket by logging on to any working computer or asking a co-worker to submit it on your behalf, and an analyst will respond in 2 hours or less.

4. **Quickr** - a Web-based application that allows the sharing of information and collaboration with groups of people inside and outside the NU domain. Both the transmission and storage of information is very secure and what level of access is granted can be managed by the data owner.
    - Appropriate for Confidential, Internal Use, or Public information.
    - Benefits and considerations of this option
    - For more information on this option, please contact your IT Account Executive or IT Product Center Manager.

5. **FTP & PGP (Pretty Good Privacy)** - highest level of confidentiality of data transmission where the data is encrypted using public/private keys and decrypted by the recipient. PGP software must be installed, licensed and supported by the external client at a small added cost.
    - Appropriate for Confidential, Internal Use, or Public information.
    - Benefits and considerations of this option
    - To request this service, the PGP Questionnaire information must be completed by the client and returned to Corporate Information Security.
    - For more information on this option, please contact your IT Account Executive or IT Product Center Manager.

View a chart comparing these options.

2.1.4. Virus Protection Procedures.

Even though IT provides anti-virus software to protect company computers, users need to be aware of what files they open. Each computer is an asset of Northeast Utilities and all users have a responsibility to protect the company's assets. Click on the following requirements for more information, or reference Virus Protection FAQs.

- Be sure that your NU computer has the latest anti-virus software and that you update it regularly by logging into the NU computer system.
- Beware of opening unrequested email attachments.
- Do not download any software from the Internet.
- Use caution when accessing personal email (i.e. Hotmail, Yahoo) at work.
- Beware of opening links to unexpected greeting cards.

2.1.5. Internet Use Procedures

The information available on the Internet can be of great business value to NU and our employees. Prudent use of this resource is needed to preserve the Company's information assets and prevent business interruption.

- Any use of the Internet that is not for specific business reasons is deemed personal use. Use of NU's Internet connection is limited to NU employees only (not "friends and family"). A commercial ISP (Internet Service Provider) such as America OnLine, Earthlink, etc. is recommended for anyone with more than occasional need for personal Internet use. Occasional use is defined as 5 hours or less per month.
- In addition to the prohibited activities referenced in the NUP 32: Use of Technology, the following Internet-specific requirements should be followed:
  - Do not listen to music stations on the Internet.
  - Use caution when accessing personal email (i.e. Hotmail, Yahoo) at work.
  - Do not download music from the Internet.
  - Close the Internet browser or navigate back to the NU Home Page after viewing external Web sites.
  - Do not violate any copyright laws when copying information or downloading files.

2.1.6. Remote Access Procedures.

Remote access refers to connecting with the NU network from a location outside the company's premises or offices. There are currently three ways of making a remote connection to the network, each with its own technical and specific security requirements:

- Virtual Private Networking (VPN)
- Internet Service Provider (ISP):
- Dial-in

Virtual Private Networking (VPN)
Using a high speed DSL or cable modem and a router, along with a laptop provided by Northeast Utilities, VPN enables faster response time and gives predictable performance similar to what you experience on the network while in the office. VPN will provide access to the Mainframe, Lotus Notes, NUnet and most NU servers via My Network Places.

Security Requirements:

1. NU Standard laptop, or an exception approved by Corporate Information Security.
2. Ensure your computer receives regular security patches and anti-virus updates.

- NU laptops should regularly log into the NU computer system (at least monthly).

3. Remote access and token from Corporate Information Security
   - See next section for requesting access

4. NU-approved VPN Client Software
   - See next section for acquiring this software

5. Router (This serves as a firewall to protect your computer while connected to the internet. The router must always be connected when using VPN.)
   - Minimum recommended model: Linksys BEFSF41

   Please click on the following links for more instructions. If you are not using the recommended Linksys router, the exact details in the links might not match, but the process is the same.

   - How to Connect the Router
   - How to Configure the Router with DSL
   - How to Configure the Router with Cable Modem

   If you have any questions, submit an ITSC Electronic Ticket by logging on to any working computer or asking a co-worker to submit it on your behalf, and an analyst will respond in 2 hours or less.

6. ISP Service (Cable Modem/DSL)

How do you get access?

NU Standard Laptop:

1. Ensure you meet all Security Requirements (section above).
2. If you do not already have remote access, complete the Create New ID/ Add Access Form and select yes at "Does the client need new Remote/VPN access?"
   - You may access this form from your Lotus Notes Welcome page via the IT Services Request link, or click here..
3. Please submit an ITSC Electronic Ticket by logging on to any working computer or asking a co-worker to submit it on your behalf, and an analyst will respond in 2 hours or less.
4. Once access has been given to your Windows 2000 User ID, please reference the VPN login instructions pamphlet to learn how to start and end Standard and Advanced VPN sessions.

Exceptions (approved by CIS):

1. Ensure you meet all Security Requirements (section above).
2. NU management must submit the Create New ID/ Add Access Form and select yes at "Does the client need new Remote/VPN access?"
   - In the ""Data to be accessed" section, include what access is needed (i.e. server name, Intranet, mainframe, Notes, etc.)
   - You may access this form from your Lotus Notes Welcome page via the IT Services Request link, or click here.
3. NU management will receive VPN software via email.

Internet Service Provider (ISP)
If you use an ISP to connect to the Internet from your home computer, then you can use the same connection to access your Lotus Notes email and calendar (iNotes). This fast, easy option is useful if you do not have a company PC or if you only need to access your email and calendar.

Security Requirements:

1. It is recommended that any non-NU computer that accesses iNotes has regular security patches and virus updates.

How do you get access?

You actually have all the access you need to connect to iNotes today. Please follow these steps:

1. While you are at the office, please register for a User ID and password if you don't have one already. The password will be mailed to you via Lotus Notes. When you receive the email, click on the link at the bottom to change your password to something that is easy for you to remember.
2. Take your User ID and password home with you.
3. At home, connect to your ISP. Go to NU's external Web site (http://www.nu.com), click on the link labeled "About NU" and then click on the link labeled "Xnet." Or, enter the address http://www.nu.com/xnet in your Web browser (you may want to create a Favorite or bookmark for this address).
4. Enter your User ID and click Continue.
5. At the "Enter Network Password" prompt, enter your User ID and password and click OK.
6. When you have completed with your work in iNotes, click on "logout" and ensure that you close the Web browser to prohibit unauthorized access to your mail.

Dial-in
Using a laptop provided by Northeast Utilities with a standard telephone (analog) line, dial-in will provide access to the Mainframe, Lotus Notes, NUnet, and NU servers (ex. K: or J: drives) at speeds up to 56,000 bits per second. Although this option is slower than using an ISP or VPN, it does give you access to all of your data on the network.

Security Requirements:

- NU Standard laptop, or an exception approved by Corporate Information Security.
- Ensure your computer receives regular security patches and anti-virus updates. NU laptops should regularly log into the NU computer system (at least monthly).
- Remote access and token from Corporate Information Security (see next section for requesting access).

How do you get access?

1. Ensure you meet all Security Requirements (section above).
2. Complete the Create New ID/ Add Access Form and select yes at "Does the client need new Remote/VPN access?"
    - You may access this form from your Lotus Notes Welcome page via the IT Services Request link, or click here.
3. Once access has been given to your Windows 2000 User ID, click on the Start button, select Dialup Connections, and click on the appropriate dial-up connection.

2.1.7. Report Suspicious Incidents.

Report instances of unauthorized use of data, fraud or suspected abuses of NU's information security policies, procedures, or guidelines to your management, Corporate Information Security, or call the BEACON line (888-NU4-0909).

2.1.8. Use of Non-NU PCs on NU's Network.

Vendors connecting to the NU network with their own PC must follow the standards below. All exceptions must be reviewed and approved by Corporate Information Security. It is ***strongly*** recommended that the NU department that the vendor is working for provides an NU PC for the vendor engagement where access is required to NU IT resources. All questions regarding compliance with these requirements should be directed to Corp Info Security.

Security Requirements:

1. **Anti-Virus Protection:** Vendor must run anti-virus software that is licensed and updated regularly.
2. **Windows Image Components:**
   - Image must be patched with latest security patches from Microsoft.
   - Image must run at least IE 6.0 SP1 with latest security patches.
   - Running the MS IIS service, operating the PC as a "server", running network monitoring tools or providing any kind of network services outside of NU (i.e., peer-to-peer software, 802.11x hardware) is PROHIBITED.
3. **Web Access:** Vendor will follow the NUP 32: Use of Technology and will only access the Internet through NU's authorized Internet connection.
4. **NU Data:** No Northeast Utilities confidential data will be stored on the vendor PC. Please refer to NUP 34: Confidential Information for more information.
5. **VPN:** VPN must be done with split tunneling disabled. This prevents a client from becoming a bridge between the NU network and a foreign "untrusted" network.
6. **Wireless:** Wireless access will be granted based on a review of business need by Corporate Information Security.

2.1.9. Use of Portable Devices and Portable Storage Media

Portable devices and portable storage media are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily transportable and can be used anywhere. As portable storage becomes more widely used, it is necessary to address security to protect information resources at Northeast Utilities. For the purposes of this procedure, portable devices and portable storage media include but are not limited to: iPods, PDAs, smart phones, thumbdrives, flash drives, memory sticks, CD / DVD, SD Cards or any externally connected mass storage device.

Requirements for use of portable storage media on Corporate Systems:
Portable storage media can be used with caution on corporate computers. The storage devices must be wiped clean and checked for viruses before use. If the portable storage media was not provided by Northeast Utilities, the origin of the device must be known to be used on Northeast Utilities computers – i.e. the device must have been purchased or provided by a reputable source. Portable storage that is "found" or has an "unknown origin" cannot be used on Northeast Utilities computers.

Confidential data on portable devices and portable storage media:
Confidential data is not allowed to be stored on any portable device or portable storage media device unless the data has been encrypted using a method approved by IT Security. See Information Handling Requirements and the Portable Device Security pamphlet for further information on protecting sensitive information.

Requirements for use of portable storage media on Critical Infrastructure:
Critical infrastructure includes CIP areas, Control Centers, Substations, Power plants, etc.

Portable storage media devices are prohibited from use in computing environments identified as or related to critical infrastructure. A special exception will be made for system administrators that need to use portable storage media devices as part of their job function.

2.2 Management Responsibilitiies

In addition to the User Responsibilities, management also has responsibility for protecting the information assets of Northeast Utilities. Management must assure that Company information is protected in a cost-effective manner because the loss or compromise of that information could adversely affect Company operations, financial condition, reputation, employees, customers or investors. Management responsibilities include the following:

1. Ensure that all employees, vendors, and contractors within the manager's area of responsibility understand their obligation to protect company information assets and to adhere to the NUP 32: Use of Technology and NUP 34: Confidential Information.

- Implement practices to protect Company confidential information as specified in this procedure.
- Establish procedures to ensure that information is accurate and free from undetected alteration.
- Provide direction regarding the release of Company information to third parties.
- Define your employee's level of "personal use" of NU's technology resources (i.e. computers, the Internet, cell phones, etc.)

2. Notify Corporate Information Security when any employee or contractor transfers or terminates.

- Reassign delegated responsibilities and access rights in a timely fashion in the event of employee transfer or termination.
- Make sure that any terminated user returns Company equipment.
- Periodically, evaluate user access to information and make sure that their level of access is appropriate.

3. Ensure that the use of information assets complies with laws and any contractual agreements.

- Ensure compliance with computer program license agreements.
- Unless specified otherwise by contract, protect proprietary information that has been entrusted to the Company by a third party.
- Clearly specify the assignment of owner and custodian responsibilities for databases, master files, and other shared collections of information that you own. Such statements must also indicate the individuals who have been granted authority to originate, modify, or delete specific types of information found in these collections of information.

4. Ensure that electronic information security requirements are met.

- Ensure that modifications to IT assets are made *only* after review and approval by an appropriate IT representative.
- Ensure that all software development and maintenance activities subscribe to Company policies and practices for systems development.
- Ensure that Company information is stored on network drives and properly backed up.

3.0 Logon Standards

These standards pertain to the use of passwords and logon IDs and to information displayed at login time for primary and secondary IT systems.

3.1 Logon Standards for Primary Systems

These standards pertain to individual user logon IDs and passwords, and to information displayed at logon time. These standards apply to:

- Systems that act as a primary connection to the NU computing environment. These systems include Active Directory Login (included in initial logon to your PC), Mainframe login, NUnet login and Remote Access.
- Users of these computer systems (i.e., employees, vendors, contractors, and agents developing and/or using company information assets); and
- Designers of these computer systems.

3.1.1 Logon Requirements for Primary Systems

The standards listed below are required for all Primary IT systems. Any exceptions to these requirements must be approved by Corporate Information Security.

1. **Logon IDs Must Uniquely Identify a Single User**For those computer and communications systems designed to support multiple users, the logon ID must uniquely identify a single user. Shared or group logon IDs are not permitted.
2. **Logon IDs Must Not Be Reused**Each computer and communications system logon ID must be unique and forever connected solely with the user to whom it has been assigned. After a user leaves the company, there should be no reuse of that logon ID.
3. **Password Minimum Length**The length of passwords should be checked automatically where possible at the time that users construct or select them. All passwords must have at least six (6) characters.
4. **Password Periodic Forced Change**All users must be automatically forced to change their passwords once every thirty to sixty (30 to 60) days.
5. **Password: Limit on Consecutive Unsuccessful Attempts to Log on**To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After six (6) unsuccessful attempts to enter a password, the involved logon ID must be either (a) suspended until reset by a system administrator, (b) temporarily disabled for a significant period of time or (c) if dial-in or other external network connections are involved, disconnected.
6. **Password and Initial Logon Process**The initial passwords issued must be valid only for the user's first on-line session. At that time, the system must require the user or instruct the user to choose another password.
7. **Password Display and Printing Prohibited**The display and printing of passwords must be masked, suppressed or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

3.1.2 Logon Guidelines for Primary Systems

The standards listed below are considered guidelines and should be used when technology allows. They are not requirements but are considered best practice for secure login.

1. **Logon IDs Must Comply With the NU Logon ID Format**The NU logon ID format is defined as the first five (5) letters of the last name, the first letter of the first name, followed by the middle initial. The resulting logon ID must be unique. The NU logon ID is currently created in the HR Corporate Person Database.
2. **Logon IDs Must Be Periodically Reviewed**At a minimum of once a year, all logon IDs must be reviewed to determine if the logon ID should remain active.
3. **Password Must Be Randomly Generated**All initial passwords to computer systems must be randomly generated. The starting point for these computations should be very difficult to predict by unauthorized parties.
4. **Password Must Be Strong** All computer system users must choose passwords that cannot be easily guessed. This means that passwords must be alphanumeric (a mix of letters and numbers) and must NOT contain your logon ID, a dictionary word or name. See Password Requirements.
5. **Password Sent Through Inter-Office Mail**When sent through the mail, passwords must be concealed inside an opaque envelope labeled "confidential" that will protect the contents and will readily reveal tampering.
6. **Password Encryption**When encryption capabilities exist, passwords must be encrypted when held in storage for any significant period of time or when transmitted over communications systems.
7. **Password Incorporated in Software**To allow passwords to be changed when needed, passwords shall not be hard-coded into software developed or modified by the company.
8. **Password Retrieval Must Be Prevented**Computer and communication systems must be designed, tested, and controlled so as to prevent the unauthorized retrieval of stored passwords.
9. **Password: Changing Vendor Default Passwords**All vendor-supplied default passwords must be changed before any computer or communications system is used for company business.
10. **Password Must Be Changed When Disclosure Suspected**All passwords must be promptly changed if they are suspected of being disclosed or known to have been disclosed to unauthorized parties. These incidences must be reported to Corporate Information Security to determine if an investigation of unauthorized use is warranted.
11. **Logon Process: Disclosure of Information in System Logon Banner**All logon banners on network-connected company computer systems must simply ask the user to log on, providing prompts as needed. Specific information about the organization, the computer operating system, the network configuration or other internal matters must not be provided in the logon banner until a user has successfully provided both a logon ID and a password.
12. **Logon Process: Security Notice in System Logon Banner**
    Every logon process on multi-user computers must include a special notice. This notice must state: (1) the system is to be used only by authorized users for authorized business purposes; (2) by continuing to use the system, the user represents that he/she is an authorized user; and (3) the user's activity is logged and monitored.
13. **Logon Process: Notice of Last Logon Time and Date**
    At log-in time if the capability exists, every user must be given information to detect unauthorized system usage including (1) the last log-in time and date; and (2) occurrence of security violations since last log-in. Corporate Information Security must be immediately informed of any suspected unauthorized usage.

3.2 Logon Standards for Secondary Systems

These standards pertain to the use of individual user logon IDs and passwords, and to information displayed at logon time. These standards apply to:

- Systems that act as a secondary connection to the NU computing environment and include all systems that are not considered primary. These systems are typically used after completing a primary connection to the NU network.
- Users of these computer systems (i.e., employees, vendors, contractors, and agents developing and/or using company information assets)
- Designers of these computer systems.

3.2.1 Logon Guidelines for Secondary Systems

Refer to the Requirements and Guidelines for Primary Systems in sections 3.1.1 and 3.1.2. These items should be considered guidelines for secondary systems and should be used when technology allows. They are not requirements but are considered best practice for secure login.

Information Security Requirements

1.0 Overview

This document provides specific requirements and other information to help in implementing Northeast Utilities' (the Company's NUP32: Use of Technology and NUP34: Confidential Information.

1.1 Purpose

Information in any form, including printed materials or electronic data, is an important asset of Northeast Utilities (the Company). The loss, corruption, and/or misuse of Company information can adversely affect the Company's operations, financial condition and reputation, as well as the interests of the Company's employees, customers and/or investors. The protection of Company information is a basic employee responsibility. Employees should consult with their management as appropriate to assure that information is protected in a manner commensurate with its sensitivity, value, and criticality, each of which may change over time. This document is not intended to interfere with an individual's rights pertaining to safety concerns.

This document provides corporate level direction for the protection of all information and information technology assets regardless of the media on which the information is stored, the systems which process it or the methods by which it is moved. While laying the cornerstone for the Company's information security architecture, this document reinforces existing Company policies and standards.

1.2 Approach

As described in the Company's NU policies, it is the policy of the Company to protect the reliability and availability of information and the security and integrity of information technology systems. This is based on a philosophy of sharing information internal to the organization. Access to certain information will be appropriately restricted based on an identifiable need to protect the information. The Company has developed, implemented, and maintains cost- effective security measures to provide authorized access to information and to prevent unauthorized access to information. For Confidential Information, the Company has in place a Confidential Information Management Program that provides oversight of the policies and procedures for the protection of Confidential Information, including these Information Security Requirements. See NUP 34.

1.3 Scope

The scope and applicability of these requirements are as follows:

- applies to all employees of the Company and its subsidiaries, as well as vendors, contractors, and agents developing and/or using Company information assets;
- applies independently of the way information is represented (e.g., written, spoken, electronic, etc.);
- applies independently of the technology used to handle the information (e.g., paper, FAX machines, computers, answering machines, cellular telephone systems, local area networks, etc.);
- applies independently of the location of information (e.g., in an office, at a customer site, on an airplane, in an employee's home, etc.); and
- protects information throughout its life cycle (e.g., origination, entry into a system, processing, dissemination, storage, disposal, etc.).

2.0 Information Handling Requirements

All Company information must be protected from unauthorized disclosure. However, some information assets are more sensitive or business critical than other information assets. This sensitive information requires special protection during a variety of processes in its life cycle, including copying and printing, shipping and manual handling, transmission by fax, phone, and electronic transmission, storage, declassification, and destruction.

To assist in determining the right level of protection for particular information and uses, Company information should be classified into one of three categories:

Confidential

Internal use

Public

Confidential - Confidential information includes personal information, confidential infrastructure information, and sensitive business information which is intended only for use by the Company or its business partner. See NUP 34. Unauthorized disclosure of this information could seriously and adversely impact the Company, its shareholders, its employees, its business partners or its customers. Confidential information requires documented access on a need to know basis, either on an individual basis or, in some cases, on a group basis. Disclosure of confidential information must be in compliance with Company policies and procedures and any additional requirements of the information owner.

Criteria to be used to identify confidential information - "Confidential information" includes the types of confidential information described in NUP 34 and may include information that:

- provides the Company with a significant competitive advantage.
- is proprietary competitive information of business partners
- shows specific business strategies and organizational directions.
- includes confidential personal information
- may be protected by laws or regulations
- is obtained through agreements that stipulate protective treatment.

Internal Use - This category applies to the majority of Company information. It includes all business- related information requiring protection from unauthorized disclosure, but failing to meet the criteria for confidential or public information. While its unauthorized disclosure is against policy, such disclosure is not expected to seriously or adversely impact the Company, its employees, its shareholders, its business partners, and/or its customers. Access to this information is implemented on a philosophy of maximized sharing within the

Company consistent with regulatory codes of conduct. Third parties may be given access to internal use information when such disclosure has been approved by management.

Examples of internal use information include:

- General correspondence
- Computer input forms (e.g., User ID Request Form)
- Production reports (e.g., MIB reports)
- NU System Telephone Directory
- General statistics (e.g., statistics from automatic call distributors in the Customer Information Centers)
- Market data from suppliers not otherwise restricted by agreement
- Administrative procedures
- Software license agreements

Public - This category applies to information that has been prepared and approved for public distribution and, as such, its disclosure will not adversely impact the Company, its employees, its shareholders, its business partners, and/or it customers. It is the responsibility of management to evaluate and approve the release of all public information. Much of this information is produced by Corporate Communications and Community Relations or is filed with governmental agencies.

Examples of public information include published items such as:

- Northeast Utilities' Annual Report
- Corporate Communications' media releases
- Consumer News
- Shareholder News
- Where NU Stands
- Integrated Resource Management Filing
- CT Siting Council Forecast of Loads and Resources

Confidential Information Definitions and Owners - Refer to NUP 34 and the Confidential Information Definitions and Owners for examples of confidential data and their owners. This may not be a complete list of data. Contact the information Owner for further clarification.

2.1 User Requirements

Every employee is required, based on the requirements described above, to determine the sensitivity of information. Based on how sensitive the information is, actions may be required to protect the information and the Company. Specifically, sensitive information must be protected with the techniques described below. If there are economic or other circumstances that suggest using alternate, equally effective protections, contact Corporate Information Security for guidance.

- Storage of Sensitive Information When Not in Use
- Transmission by Phone, FAX, and via the Internet
- Shipping and Manual Handling
- Labeling
- Declassification
- Copying and Printing
- Disposal of Sensitive Information
- Handling Sensitive Data in Meetings
  Granting Access to Sensitive Data

- Physical Security
  - Protection of Sensitive Information Off Company Premises
  - Protect all Company Information from Unauthorized Disclosure

Refer to the Confidential Information Seven Key Practices for a summary of these handling requirements.

Storage of Sensitive Information When Not in Use

When not being used by authorized users, all hard copy sensitive information shall be locked in file cabinets, desks, safes or other office furniture. Likewise, when not being used, all computer media (e.g., floppy disks, tapes, CD- ROMs, etc.) containing sensitive information shall be locked in similar enclosures.

Transmission by Phone, FAX, E-Mail, and via the Internet

1. Use of Cordless or Cellular Phones for Confidential Discussions –Sensitive information shall not be discussed on cordless or cellular telephones. If discussion of such information is required, users shall use guarded terms and refrain from mentioning confidential details beyond those absolutely required to get the job done.

2. Use of Speaker- Phones for Sensitive Discussions –Sensitive information shall not be discussed on speaker- phones, unless both the source and the recipient state at the beginning of the conversation that no unauthorized persons are in a position where they might overhear the conversation at either the source's or the recipient's location.

3. Leaving Sensitive Information on Phone Answering Machines or Voice Mail Systems - Users shall refrain from leaving messages containing sensitive information on answering machines or voice mail systems, unless assurance has been provided in advance that the recipient's messages have reasonable security measures in place, i.e., password protection. This protection will help ensure that the information is communicated only to the intended party.

4. Use of FAX Machines –Sensitive information may be FAXed in an unencrypted format only when both: (1) time is of the essence and (2) no alternative and higher- security transmission methods are available. In these instances, to ensure that information is not disclosed to unauthorized parties, voice contact with the receiving party shall be established immediately prior to transmission or it shall be established with the receiving party that the receiving FAX machine is password protected.

5. Sensitive Information Sent by Internal E-Mail - Sensitive information sent by internal e-mail (from a company Lotus Notes account to a company Lotus Notes account) shall be labeled Confidential. The sender shall select the 'Mark Subject Confidential' Mail Option, which will add ***Confidential:** to the beginning of the e-mail subject line.

6. Sensitive Information Sent Electronically Over the Internet –Consideration shall be given to the sensitivity of information before sending it over the Internet, and encrypted transmittal is mandatory for sensitive information. The following methods are presently available to exchange information electronically with external parties. Each providing different levels of information protection (not all are suitable for sensitive information) and capability for dealing with large file sizes:

Benefits

	available to third parties	small file size (5 meg)	large file size (5 meg)	lengthy relationship with 3rd party (6 months)	dynamic 3rd parties (6 months)	encrypted transmittal	secure storage
Technology							
Lotus Notes email	x	x			x		x
NU's FTP	x		x	x	x		x
WinZip/email	x	x			x	x	x
WinZip/FTP	x		x	x	x	x	x
Quickr	x	x	x	x		x	x
FTP & PGP			x	x		x	x

a. **Lotus Notes E- mail** - transmission of e-mail over the Internet is text- based (or "clear" text) and could be obtained by a third party.

Benefits

E- mail is easy to use and, next to the telephone, is one of the most widely accepted forms of electronic communication. It is a continuously growing medium for transacting business as more companies continue to make themselves accessible through Internet. Most of the time, e- mail messages are short in text length and are received instantaneously. NU- IT provides virus protection on all inbound and outbound e- mails and any associated attachments. :

NU appends the following disclaimer on all outbound e- mail:

> This e-mail, including any files or attachments transmitted with it, is confidential and intended for a specific purpose and for use only by the individual or entity to whom it is addressed. Any disclosure, copying or distribution of this e- mail or the taking of any action based on its contents, other than for its intended purpose, is strictly prohibited. If you have received this e- mail in error, please notify the sender immediately and delete it from your system. Any views or opinions expressed in this e- mail are not necessarily those of Northeast Utilities, its subsidiaries and affiliates (NU). E- mail transmission cannot be guaranteed to be error- free or secure or free from viruses, and NU disclaims all liability for any resulting damage, errors, or omissions.

Considerations

Since e- mail transmission is in "clear" text, it is considered a very insecure mechanism of communication. Delivery of e- mail cannot be guaranteed plus its contents could be intercepted, copied and modified without the recipient's knowledge. It's possible that the custodian of the electronic transmission media could read an e- mail. Any Internet Service Provider and other carriers used along the transmission path as well as certain IT personnel within the sending and receiving companies have the ability to intercept e- mails.

Due to the current pervasive problems with unsolicited e- mail, many companies have implemented filters which either can delay or completely stop the delivery of

certain e- mails. Also, e- mails with large file attachments (i.e., over 5 megabytes) are at risk of not being received because of these same filters or because of space limitations on the recipient's email account. Therefore, other procedural controls may need to be put in place to help ensure the integrity of a critical e-mail either sent to or received from an external party.

For instructions on how to implement this service, refer to the IT Corporate Information Security Procedure.

b. **File Transfer Protocol (FTP)** - transmission of data over the Internet is text-based (or "clear" text) and could be obtained by a third party. Although the information in transit is not secure, the temporary storage area from where the file is to be retrieved is protected.

Benefits

The FTP (File Transfer Protocol) service is designed specifically for large file exchanges (more than 5 megabytes). FTP uses the internet/intranet to copy files very quickly from one computer to another regardless of distance either within NU's network or to any third party that has Internet access. This method eliminates the need for large file attachments in emails and is a more reliable delivery method. A secure temporary storage area is defined for FTP use. This is the preferred method of transfer for large files (5 Megabytes or greater) to people outside the company. Virus protection is provided on the FTP server to protect against viruses, and user activity is monitored on NU's FTP server by Corporate Information Security (CIS).

Depending on the need, there are two different ways to engage external parties in using NU's FTP services:

- clients that exchange large files frequently over a long duration but with only 1 or 2 external parties and
- clients that exchange large files infrequently but with many external parties.

Considerations

FTP transmission of files is also in "clear" text and susceptible to some of the same risks described for the e- mail option above.
For instructions on how to implement this service, refer to the IT Corporate Information Security Procedure.

c. **Using password protection for WinZip Files** - data is compressed or "zipped" then password protected before transmission, then password challenged and "unzipped" by the recipient upon a successful transmission. This method provides an improved level of protection since using a password encrypts the file and protects it from the casual eavesdropper. This option may be used with e-mail or FTP.

Benefits

Any type of file can be compressed or "zipped" by the client, or "zipped", using the WinZip utility. This utility is now available on every Windows 2000 PC and prevents the transmission of data in clear text over the Internet. Generally,

zipping a file reduces storage and transmission requirements and, in some cases, can reduce the file size up to 80%. Password protecting files in a "zipped" format provides an added measure of protection against users who do not have the password and are trying to determine the contents of your files.

Sending password protected "zipped" files via e- mail or FTP provides the same benefits as described under Options 1 and 2 plus it eliminates the risks associated with "clear text" transmissions.

Considerations

Due to the continuous threat of viruses, many companies have implemented policies that prevent employees from receiving "zipped" files via e- mail from the Internet. It is important that you contact the external party to confirm whether such a policy is in place before using this option.

Also, an agreed upon convention must be established with the external party for developing and exchanging the WinZip password. This password must be communicated via another medium (i.e., a telephone call) and should not be included in the e- mail that contains the "zipped" file.

Although password protecting a "zipped" file uses a form of encryption, the level of encryption utilized may still not meet a contractual obligation or certain legal requirements. Some laws are very specific as to what is an acceptable level of encryption that must be used for either storing or transmitting specifically defined information. To obtain clarification on these requirements, please consult with the information owners identified in the Confidential Information Definitions and Owners 85KB.

For instructions on how to implement this service, refer to the IT Corporate Information Security Procedure.

d. **Quickr -** a Web-based application that allows the sharing of information and collaboration with groups of people inside and outside the NU domain. Both the transmission and storage of information is very secure and what level of access is granted can be managed by the data owner.

Benefits

Quickr should be used when you have a business activity that involves sharing information and collaboration with groups of people within one or several external organizations. It is an easy-to-use web-based product accessible on NU's external web site that is installed on a protected server where all communication is encrypted and access is controlled for every user. It is very similar to a discussion database or document library in its operation but has an added benefit of having "rooms". A room is like a folder with security on it to control who has access and what they can do in each room.

Documents can be posted and retrieved from these rooms or they can be worked on collectively. E-mail notification may be used to advise users when a new document has been posted or any other changes within their defined work "rooms". It also has calendaring capabilities to remind users of key events (i.e., project deadlines).

Considerations

Each room requires an administrator that defines and controls access to its folders and pages for both internal and external users. Each user needs a logon-id and password defined by the administrator. Costs associated with Quickr includes licenses for NU users only, approximately $30 per user annually.

To request a Quickr for your project, send an email to Notes Administrator (adminn@nu.com).

e. **FTP & PGP (Pretty Good Privacy)** - highest level of confidentiality of data transmission where the data is encrypted using public/private keys and decrypted by the recipient. PGP software must be installed, licensed and supported by the external client at a small added cost.

Benefits

This option provides the highest level of information integrity protection and security and should be used when there exists a legal or regulatory requirement, or contractual obligation to use strong encryption to either send or receive information via the Internet with an external party. The remaining benefits are the same as those described under Option 2 for FTP.

Considerations

Because of the relatively high maintenance effort required to implement FTP with PGP, this option should be used with external parties where NU has a long- term relationship (i.e., more than 6 months). Also, it is to be used only for pre- defined, automated transfers (i.e., the same file every month) at scheduled intervals. Working in conjunction with FTP, a file is encrypted by the sending company and decrypted by the receiving company using the PGP application. To initially establish this process, this option requires involvement from both internal and external IT support staff to build and test the transfer process. The ongoing IT maintenance and support costs are minimal.

For instructions on how to implement this service, refer to the IT Corporate Information Security Procedure.

Shipping and Manual Handling

When assessing the following, contact the information owner to determine the most effective practices to be implemented.

1. Tracking Copies of Sensitive Information - Whenever there are multiple copies of sensitive information, number each copy of the document and record the recipient of each copy in a log maintained by the information custodian.

2. Envelopes For Sensitive Information Sent by Internal or External Mail - In general, sensitive information shall be sent through internal or external mails in a sealed opaque envelope labeled Confidential: To Be Opened By Addressee Only .
   Where additional protection is warranted, sensitive information shall be sent

through internal or external mail in a sealed opaque envelope labeled Confidential: To Be Opened by Addressee Only, which is in turn enclosed in a plain outer envelope or interoffice envelope.

3. Recommended Method for Sending Sensitive Information Via External Mail - Consider sending sensitive information in hard copy form by registered mail.

4. Acknowledgement Required for Deliveries of Sensitive Information - Deliveries of sensitive information shall be acknowledged by the recipient within a pre- established period of time.

Labeling

1. Sensitive information Labeling Requirements - Hardcopy confidential information, i. e. certain computer reports, forms, memos, etc., shall be labeled Confidential.

2. Labeling of Confidential Hard Copy - All printed or handwritten copies of sensitive information shall be labeled Confidential on the upper right hand corner of each page or, if bound, on the front cover, the title page, and the rear cover.

3. Floppy Disk Labeling Requirements - All floppy disks containing confidential information shall be externally labeled Confidential.

Declassification

1. Declassification Date for Sensitive Information Part of Label - Whenever applicable and technically feasible, the date that sensitive information will no longer be considered confidential shall be indicated as part of the label. Specifically, the document originator shall determine the date when protection will end and mark the document accordingly, for example, Confidential Until (date).

2. Declassification of Sensitive Information Required as Soon as Practical - From the standpoint of sensitivity and cost, sensitive information shall be declassified (i.e., downgraded) as soon as practical.

Copying and Printing

1. Permission Required When Making Copies of Sensitive Information - Making additional copies or printing extra copies of sensitive information shall not take place without the advance permission of the information owner.

2. Destruction of Intermediate Products Containing Sensitive Information - If a copy machine or printer jams or malfunctions while making copies of sensitive information, the user shall not leave the machine until all copies of the information are removed from the machine and shredded.

3. Attended Operation Required When Printing Sensitive Information - Printers shall not be left unattended if sensitive information is being printed or will

soon be printed. Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorized to see the material being printed may not enter or the output is sent to a password protected mailbox.

4. Third Party Non- Disclosure Agreements and Sensitive Information - Prior to sending sensitive information to a third party for copying, printing, formatting or other handling, consideration shall be given to having the third party sign a Northeast Utilities non-disclosure agreement.

Disposal of Sensitive Information

1. Disposal of Drafts - Information shall be destroyed when it is no longer needed. Only current drafts of a document should be maintained, unless specific practice or regulation requires that all versions of a document be maintained.

2. Use of Secure Locations to Store Sensitive Information to Be Destroyed - All sensitive information that is no longer being used or that is no longer needed- no matter what form it takes (disks, hardcopy, etc.)—shall be placed in a secure locations until such time as authorized Company personnel or a bonded destruction service picks it up for destruction.

3. Approved Methods for Hardcopy Sensitive Information Disposal - When disposing of sensitive information in hard copy form (e.g., paper, microfilm, microfiche, etc.), it shall be shredded.

4. Destruction of a Sensitive Information File on Computer Storage Media – Consideration shall be given to the use of special technology to delete sensitive files. Merely deleting a file will, in most cases, not result in deleting the information; i. e. it may still be retrievable. For storage media controlled by others, i.e., servers or mainframe, if information is deleted before the backup is run, it will be deleted. If information is deleted after the backup is run, this information will be retrievable for the length of the backup cycle, i.e., several weeks.

Handling Sensitive Data in Meetings

If sensitive information is released orally in a meeting, seminar or related presentation, the speaker shall clearly communicate the confidentiality of the information and its owner. The speaker shall also remind the audience not to disclose this information to others, unless approved by the information owner. Visual aids such as slides and overhead transparencies shall be labeled Confidential.

Granting Access to Sensitive Data

1. Approval Required Before Access to Sensitive Information - Access to sensitive information shall be granted only after express management authorization from the information owner or designee has been obtained.

2. Use of Access Control Throughout Sensitive information's Life Cycle - If sensitive information previously resident on a mainframe is down- loaded to

a microcomputer, access controls shall be consistent as the information's form, location, and presentation changes.

Physical Security

Physical Access Control for Areas Containing Sensitive Information - Access to every office, computer room, and work area containing sensitive information shall be physically restricted. Management responsible for the staff working in these areas should consult the Corporate Security Department to determine the appropriate access control method (e.g., receptionists, metal key locks, card readers, etc.).

Protection of sensitive Information Off Company Premises

1. Removal of Sensitive Information - The intention of this requirement is to ensure that residual information which may have been erased is not left on the storage media and therefore recoverable by a third party. Before computer magnetic storage media is returned to a vendor for trade-in, servicing or disposal, all sensitive information shall be removed according to methods approved by the Corporate Information Security Department.

   All computer storage media sent from the Company to a third party shall be new, or if used, shall be degaussed prior to recording the information intended to be transferred.

2. Storing Sensitive Information on Transportable Computers - Users in possession of portable, laptop, notebook, palmtop, and other transportable computers containing sensitive information shall ensure that device has been encrypted by a technology approved by Corporate Information Security.
3. Use of Sensitive Information Off Company Premises - Users in possession of hardcopy sensitive information that is taken off company premises for business use (e.g., telecommuting, travel to other company work locations, etc.) shall ensure the information is protected at all times. When the documents are in use, the user shall adhere to all established measures and precautions to ensure that unauthorized persons do not gain access to the sensitive information. When the documents are not in use, they shall be kept out of site, and in a locked location (e.g., hotel room, home, vehicle, etc.).

Protection of company information from unauthorized disclosure

- Verify that the disclosure of company information has been approved by management.
- Verify that the disclosure of sensitive information has been approved by the information owner.
- Verify the identity of the requester and that they have an authorized need for the information.
- Company information shall not regularly be stored on the hard disk drive or other internal components of a personal computer. Information shall be stored on the network drives to ensure that regular backups of the data occur. In instances where temporary storage of sensitive information on the hard disk drive is necessary, the files shall be stored in the "My Documents" folder, which has an extra layer of password protection.

2.2 Management Requirements.

In addition to the User Requirements, management also has responsibility for protecting the information assets of Northeast Utilities. Management must assure that Company information is protected in an effective and cost-effective manner because the loss or compromise of that information could adversely affect Company operations, financial condition, reputation, employees, customers or investors. Requirements applicable to Management include the following:

1. Ensure that all employees, vendors, and contractors within the manager's area of responsibility understand their obligation to protect company information assets and to adhere to the NUP 32: Use of Technology and NUP 34: Confidential Information.

    - Implement practices to protect Company sensitive information as recommended in this procedure
    - Establish procedures to help ensure that information is accurate and free from undetected alteration.
    - Provide direction regarding the release of Company information to third parties.
    - Define employee's level of "personal use" of NU's technology resources (i. e. computers, the Internet, cell phones, etc.)

2. Ensure that all information assets in the manager's area of responsibility are properly protected.

    - Ensure that the assignment of ownership and custodian responsibilities for the shared collection of information has been clearly delegated.

2. 3 Owner/Custodian Requirements

- Owner - The owner (i.e., a vice president or above or their designee) shall identify and protect all information assets received by or generated within his or her assigned area of management control in compliance with Company policies and procedures for such Information.
- The owner shall assess the degree of risk involved with ensuring information security, reliability, and availability and determine if adequate controls are in place to mitigate such risks, including participation in the development of a Business Resumption Plan.
- The owner shall assume ultimate responsibility for the proper classification, use, and protection of information the organizational unit owns and uses in compliance with Company policies and procedures for such Information.
- The owner shall, in order to facilitate proper protection, assign responsibility and accountability for protecting each major information asset, regardless of media, to an information custodian.
- Unless applicable law provides sufficient protection, the owner shall take measures to ensure that all disclosures of sensitive information outside of the owner's business organization are accomplished in accordance with Company policies and procedures for the confidentiality and protection of such Information and any disclosures to contracted agents or third parties are accomplished via an appropriate executed agreement that includes restrictions on the subsequent dissemination and usage of the information.
- The owner shall take measures to ensure that data processing suppliers outside the Company provide adequate physical and procedural safeguards

to ensure that access to sensitive information stored in their computers (i.e., including all magnetic media) is controlled as prescribed by the owner of the information.

Custodian - The custodian shall implement and maintain cost-effective information control measures, consistent with the instructions of the information owner and requirements from Corporate Information Security.

- The custodian shall provide physical safeguards for mainframe, network environments, and all other forms of information.

The custodian shall set the rules for information access and usage and grant access to the users who have been authorized by the information owner.

APPENDIX G

ATTACHMENT D

ISO New England Information Policy

Table of Contents

Introduction

The ISO New England Information Policy establishes rules and guidelines regarding the appropriate disclosure of all information received, created and distributed in connection with the operation of and participation in the markets administered by ISO New England Inc. (the "ISO"). The Policy allows stakeholder committees, task forces and working groups (collectively, "Stakeholder Committees"), the ISO, and Governance Participants to share information with the benefit of a common understanding regarding how that information will be used and how appropriate confidentiality will be maintained. This Policy document consists of three sections. Section 1 highlights the Policy's intent and objectives. Section 2 discusses confidentiality issues. Finally, Section 3 specifies what types of information are available to whom. This Section, in its entirety, is intended to replace the Information Classification Document appendix of the formerly adopted Policy (March 5, 1999 version).
Changes to the Information Policy will be made in accordance with Section 11.3 of the Participants Agreement.

Section 1 -Policy Intent & Objectives

The intent of this Policy is twofold. First, to allow Governance Participants to provide certain *Confidential Information* to the ISO, Stakeholder Committees, and other Governance Participants with the benefit of a common understanding regarding how that information will be used and how appropriate confidentiality will be maintained. Second, to provide the ISO, Stakeholder Committees and Governance Participants clear guidance regarding the appropriate disclosure of all information received, created or distributed in connection with the operation of and participation in the markets administered by the ISO. This Policy will pertain to all information held by Stakeholder Committees or the ISO, or furnished by or to a Governance Participant as a result of its participation in the markets administered by the ISO, whether it is publicly available or strictly confidential.

In order to meet the general obligations of the Transmission, Markets and Services Tariff, the Participants Agreement, the Transmission Operating Agreement, the Rates Design and Funds Disbursement Agreement, and other documents that affect the rates, terms, and conditions of service, including all exhibits and attachments to the listed documents (hereafter collectively referred to as the "Filed Documents"), each Governance Participant is required to furnish to and may be entitled to receive from Stakeholder Committees or the ISO certain information, some of which may be considered confidential, commercially sensitive, and/or strategic in nature. This information is used by the ISO, Stakeholder Committees or Governance Participants, as appropriate, for the following purposes, among others:

1. To operate the bulk power supply system on a day-to-day basis.

2. To administer the Open Access Transmission Tariff.

3. To administer the New England electricity markets, including the bidding process, billing system and settlement function.

4. To monitor the competitiveness and efficiency of the market and Governance Participants' compliance with relevant market rules and procedures.

5. To assess and plan for the long term reliability and adequacy of the New England bulk power supply system.

6. To provide reports and data as required or appropriate to the various user groups as described in Section 3 of this document.

It is recognized that the successful operation of the New England Control Area is highly dependent on access to certain types of information. The high degree of bulk power supply reliability and adequacy that customers of Governance Participants have become accustomed to expect is, to some degree, a result of Governance Participants' willingness to provide the necessary information. It is only with the ISO's continued access to the information necessary to perform its duties described above that the benefits obtained from bulk power supply pooling can continue.
This Information Policy will:

1. Recognize that protecting the confidentiality of certain information is important to the Governance Participants.

2. Recognize that the ISO and each Governance Participant have the responsibility to protect the confidentiality of such information.

3. Provide procedures and guidelines to the ISO, Stakeholder Committees and Governance Participants regarding the handling, publication and distribution of all information.

This Information Policy is intended to comport with the obligation of the ISO, Stakeholder Committees and the Governance Participants to comply fully with the antitrust laws and the information access and disclosure provisions of the standards of conduct promulgated by the Federal Energy Regulatory Commission in 18 C.F.R. § 37.4 (the "Codes of Conduct"). The Information Policy is expressly intended both: **(1)** to protect against the disclosure of *Confidential Information* that could facilitate anticompetitive conduct prohibited by the antitrust laws and **(2)** to distribute information to the extent and in a manner consistent with preserving the competitiveness and efficiency of the New England electric markets and the reliability of the bulk power system.

No modifications or additions shall be made to Section 3 of this document that result in limiting the disclosure of *Confidential Information* by Governance Participants that are municipalities, state or municipal agencies, or other public agencies unless such information contains trade secrets or commercial or financial information that has otherwise been kept confidential.

Section 2 -Confidentiality Issues

2.0 Confidentiality

Confidential Information furnished by a Governance Participant to Stakeholder Committees and/or the ISO shall, for the purposes of this Information Policy, be considered the sole and exclusive property of such Governance Participant (the "Furnishing Governance Participant"). To the extent that such *Confidential Information* is furnished to Stakeholder Committees and/or the ISO it shall be used solely to perform their obligations under the NEPOOL Agreement and the ISO Agreement. No Governance Participant shall be entitled to receive from the ISO and/or Stakeholder Committees any *Confidential Information* furnished by another Governance Participant under the NEPOOL Agreement unless the Furnishing Governance Participant has provided the relevant Stakeholder Committees and/or the ISO written authorization for such release. The disclosure of *Confidential Information* in accordance with this Information Policy shall not be used by any Governance Participant as a basis for a claim that the Governance Participant furnishing such *Confidential Information* has waived, relinquished, or reduced in any way the Furnishing Governance Participant's rights to prevent further disclosure of such *Confidential Information.*

The Governance Participants recognize that one of the purposes of the ISO is to prepare analyses, forecasts and reports for the general public, reliability councils, regulators and other user groups.

Preparation of such analyses, forecasts and reports requires the use of Governance Participants' information, some of which may be *Confidential Information* of an individual Governance Participant.

Governance Participants' obligations to provide information to the ISO or Stakeholder Committees arise under the Filed Documents. Nothing in this Information Policy is intended to expand or alter those obligations. Nothing in this Information Policy requires the ISO to release information to Stakeholder Committees, Governance Participants or any other person if the ISO in good faith believes that the release of such information would violate any applicable law or regulation, including the Codes of Conduct, or the terms of any valid confidentiality agreement or have a material adverse effect on the competitiveness or efficiency of the markets administered by the ISO.

2.1 Confidential Information

The following information will be considered *Confidential Information* for the purposes of this Policy:

(a) Information that **(i)** is furnished by a Governance Participant (the "Furnishing Governance Participant") to the ISO, Stakeholder Committees or another Governance Participant, **(ii)** constitutes trade secrets or commercial or financial information, the disclosure of which would harm the Furnishing Governance Participant or prejudice the position of that Governance Participant in the New England electricity markets, and **(iii)** has been designated in writing by the Furnishing Governance Participant as confidential or proprietary either in the document which provided such information, in the transmittal materials accompanying such information, or in a separate document which identifies the information with sufficient specificity and clarity so that the entity receiving such information has been made aware that the Furnishing Governance Participant seeks confidential treatment for such information.

(b) Information that **(i)** is furnished by the ISO to a Governance Participant or a Stakeholder Committee, **(ii)** constitutes trade secrets or commercial or financial information the disclosure of which would have an adverse effect on the ability of the ISO to perform its responsibilities under the ISO Agreement, and **(iii)** has been designated in writing by the ISO as confidential or proprietary either in the document which provided such information, in transmittal materials accompanying such information, or in a separate document which identifies the information with sufficient specificity and clarity so that the entity receiving such information has been made aware that the ISO seeks confidential treatment for such information. In addition, information that is furnished by the ISO to a Governance Participant or a Stakeholder Committee relating to the

job status or performance or terms of employment of any ISO employee ("ISO Employment Information") shall be *Confidential Information.*

(c) Information that **(i)** is furnished by a non-Governance Participant that takes part in a demand response program operated by the ISO (a "DR Information Provider") to the ISO, Stakeholder Committees or any Governance Participant in connection with the demand response program, **(ii)** constitutes trade secrets or commercial or financial information, the disclosure of which would harm the DR Information Provider or prejudice the position of the DR Information Provider in the demand response program, and **(iii)** has been designated in writing by the DR Information Provider as confidential or proprietary either in the document which provided such information, in the transmittal materials accompanying such information, or in a separate document that identifies the information with sufficient specificity and clarity so that the entity receiving such information has been made aware that the DR Information Provider seeks confidential treatment for such information.

(d) Information that **(i)** is furnished by a non-Governance Participant acting as a Project Sponsor to the ISO, Stakeholder Committees or any Governance Participant in connection with the Forward Capacity Market, **(ii)** constitutes trade secrets or commercial or financial information, the disclosure of which would harm the Project Sponsor or prejudice the position of the Project Sponsor in the Forward Capacity Market, and **(iii)** has been designated in writing by the Project Sponsor as confidential or proprietary either in the document which provided such information, in the transmittal materials accompanying such information, or in a separate document that identifies the information with sufficient specificity and clarity so that the entity receiving such information has been made aware that the Project Sponsor seeks confidential treatment for such information.

(e) Information disclosed to satisfy the "Minimum Criteria for Market Participation" set forth in Section II.A of the ISO New England Financial Assurance Policy that (i) is furnished by a Furnishing Governance Participant to the ISO, Stakeholder Committees or another Governance Participant or is furnished by the ISO to a Governance Participant or a Stakeholder Committee, (ii) constitutes sensitive or non-public information concerning the Participant or identifying or concerning the Principals of a Participant, the disclosure of which could harm the Furnishing Governance Participant or its Principals, and (iii) has been designated in writing by the Furnishing Governance Participant or by the ISO as confidential either in the document which

provided such information, in the transmittal materials accompanying such information, or in a separate document which identifies the information with sufficient specificity and clarity so that the entity receiving such information has been made aware that the Furnishing Governance Participant or the ISO seeks confidential treatment for such information.

(f) Any report, compilation or communication produced by the ISO or a Stakeholder Committee that contains information described in Clause (a), (b), (c), (d) or (e) above and allows for the specific identification of the Furnishing Governance Participant or the DR Information Provider.

Confidential Information shall exclude information if and to the extent such information **(1)** is or becomes generally available to the public without any party violating any obligation of secrecy relating to the information disclosed, or **(2)** is received by a Governance Participant in good faith from a third party who discloses such information on a non-confidential basis without violating any obligation of secrecy relating to the information disclosed, or **(3)** is defined as "Public Information," in Section 3, or **(4)** can be shown by the recipient's prior records to have been already known to the recipient other than through disclosure by a third party which would not be subject to exclusion based on (2) above.

Confidential Information, as defined in this Section 2.1, may be provided to specific user groups entitled to information pursuant to Sections (a) through (i) of Section 3.0. Section 3.0 is not intended, however, to add to or vary the criteria specified above. Otherwise, except as specifically provided herein, no other distribution or disclosure of *Confidential Information* shall be permitted by the ISO, Stakeholder Committees or Governance Participants.

2.2 Treatment of Confidential Information

The Governance Participants shall take reasonable measures to assure that all of their employees, representatives, or agents who by virtue of their participation on, or as an alternate on, a Stakeholder Committee have access to *Confidential Information* of another entity that furnished the information, including, as appropriate, a Furnishing Governance Participant, a DR Information Provider or the ISO (the "Furnishing Entity") (1) do not disclose such *Confidential Information* to any other employee, representative, or agent of the same Governance Participant or any other person except as permitted under this Section 2.2 and (2) use such information solely for the purpose of satisfying that person's responsibilities on the Stakeholder Committee. Each Governance Participant shall, upon request by the Participants Committee, provide assurance that the terms of this Section 2.2 are complied with. Any Governance Participant that has furnished *Confidential Information* to Stakeholder Committees may

require each recipient to return all or any portion of the *Confidential Information* once it is no longer needed by such recipient to fulfill its responsibilities under the Filed Documents.

Notwithstanding the foregoing, the ISO, the Participants Committee or any Governance Participant may disclose *Confidential Information* of another Governance Participant or the ISO only: **(1)** if such disclosure is permitted in writing by the Furnishing Entity, DR Information Provider or the ISO, as the case may be, or **(2)** if disclosure is required by order of a court or regulatory agency of competent jurisdiction or dispute resolution pursuant to the Filed Documents, or **(3)** as otherwise specifically permitted by this Policy. Any entity subject to this Information Policy shall provide prompt written notice to the Furnishing Entity if that entity either is compelled by order of a court or regulatory agency of competent jurisdiction to disclose, or receives a request seeking to compel disclosure of, *Confidential Information* for which it is not the Furnishing Entity. Further, in recognition that certain Governance Participants are subject to public records and open meeting laws and that certain other demands may be placed on Governance Participants to disclose *Confidential Information*, a recipient of *Confidential Information* of another Governance Participant or the ISO may disclose such *Confidential Information* if and to the extent required by law or requested in writing pursuant to a public records demand or other legal discovery process, provided in either event that the disclosing Governance Participant gives the Furnishing Governance Participant or the ISO prompt written notice of the circumstances that may require such disclosure in time so that the Furnishing Governance Participant or the ISO has a reasonable opportunity to seek a protective order to prevent disclosure.

Notwithstanding anything to the contrary contained in this Section 2.2, the ISO, the Participants Committee, or any Governance Participant may disclose *Confidential Information* to an alternate dispute resolution ("ADR") neutral in an ADR proceeding required or permitted by any New England market rule, including Appendix A, "Market Monitoring, Reporting and Market Power Mitigation," and Appendix B, "Imposition of Sanctions," to Market Rule 1, or to an arbitrator in an arbitration proceeding under the Filed Documents. In addition, the ISO or any Governance Participant may disclose *Confidential Information* to a Dispute Representative as defined in, and permitted by, Section 5 of the Billing Policy. Any such ADR neutral, arbitrator or Dispute Representative must agree to be bound by this Information Policy.

Notwithstanding anything to the contrary in this Information Policy, resource-specific information contained in the data fields of the Forward Capacity Tracking System, but not information provided to the

ISO as separate attachments via the Forward Capacity Tracking System, will be shared with subsequent Lead Market Participants or Project Sponsors for that resource.

Notwithstanding anything to the contrary in the ISO New England Information Policy, the ISO, the Participants Committee, or any Governance Participant may disclose *Confidential Information* as required or permitted to satisfy the "Minimum Criteria for Market Participation" set forth in Section II.A of the ISO New England Financial Assurance Policy.

Notwithstanding anything to the contrary in the ISO New England Information Policy and consistent with FERC Order 787, the ISO may disclose *Confidential Information* concerning natural gas-fueled generation from resources located within the New England Control Area to the operating personnel of an interstate natural gas pipeline company that operates a pipeline provided that: (a) *Confidential Information* regarding specific generators will be shared only with the pipeline serving that generator directly and (b) the ISO has determined that it is operationally necessary to ensure reliability to disclose the *Confidential Information.*

2.3 Disclosure of Information Regarding Defaulting Governance Participants

Notwithstanding any provision herein to the contrary, the information for release to Governance Participants identified in this Section shall no longer be deemed "*Confidential Information*" pursuant to the Information Policy. For any Governance Participant that is the subject of a voluntary or involuntary bankruptcy petition or has sought relief under bankruptcy or insolvency laws, or that has otherwise defaulted under its arrangements with the ISO, which default is not, or the ISO reasonably concludes will not be, cured within five days of the date of the default, in the case of a Payment Default (as defined in the Billing Policy) or within ten days of the date of its default in the case of any other defaults, the following information with respect to that Governance Participant's obligations shall be disclosed by the ISO to each member and alternate on the Participants Committee, each Governance Participant's billing contacts, appropriate Stakeholder Committee(s) designated by the Participants Committee, and appropriate state regulatory or judiciary authority:

> For the 60 calendar day period prior to the date of the bankruptcy, insolvency petition or other default (the "Default Date") and from the Default Date forward until such time as the Governance Participant cures the default: **(i)** the type and available amount of financial assurance in place; **(ii)** any notification provided by such Governance Participant pursuant to the Financial Assurance Policy and/or Billing Policy to the ISO of a material change in its financial status; **(iii)** any change

in the type or available amount of financial assurance provided by such Governance Participant; **(iv)** whether such Governance Participant has defaulted on its payment obligations under the Billing Policy, the amount of any such default, the date of the default, and when or whether the default is cured; **(v)** whether such Governance Participant has defaulted on its obligations under the Financial Assurance Policy, the amount of any such default, the date of the default, and when or whether the default is cured; **(vi)** where the financial assurance provided by such Governance Participant is a bond, whether the ISO has provided notice of default to the surety and whether the surety has given notice of termination of the bond or otherwise disclaimed or refused to honor or delayed in honoring its obligations under the bond, and the response of the ISO to any such notice; **(vii)** whether such Governance Participant is a net seller or purchaser in the New England Markets; **(viii)** the amount of such Governance Participant's purchases in the New England Markets; and **(ix)** whether such Governance Participant owns a registered Load Asset.

If a Governance Participant is suspended from the New England Markets, the ISO immediately shall send notice of such suspension to each of the members and alternates on the Participants Committee, the energy regulatory agencies in each of the New England states and the Federal Energy Regulatory Commission. Said notice shall identify the specific date and time of the suspension.

2.4 Breach of Confidential Information Obligations

The Governance Participants and the ISO acknowledge that remedies at law for any breach of the obligations under this Section 2 would be inadequate and agree that, in enforcing this Section 2, in addition to any other remedies provided at law:

(a) A Furnishing Governance Participant may, at its option, take one or both of the following actions: **(i)** apply to any court of equity having jurisdiction for an injunction restraining the ISO, any Stakeholder Committee or any Governance Participant from an actual or threatened violation of this Section 2 relating to *Confidential Information* provided by such Furnishing Governance Participant and **(ii)** submit such actual or threatened violation to arbitration in accordance with the procedure provided in Section 17.3 of the Participants Agreement and Section I of the Transmission, Markets and Services Tariff.

(b) The ISO may, at its option, take one or both of the following actions: **(i)** apply to any court of equity having jurisdiction for an injunction restraining a Governance Participant or any Stakeholder Committee from an actual or threatened violation of this Section 2 relating to

Confidential Information and **(ii)** submit such actual or threatened violation to arbitration in accordance with the procedure provided in Section 17.3 of the Participants Agreement and Section I of the Transmission, Markets and Services Tariff.

(c) The Participants Committee may, at its option, take one or both of the following actions: **(i)** apply to any court of equity having jurisdiction for an injunction restraining the ISO from an actual or threatened violation of this Section 2 relating to *Confidential Information* and **(ii)** submit such actual or threatened violation to arbitration in accordance with the procedure provided in Section 17.3 of the Participants Agreement and Section I of the Transmission, Markets and Services Tariff.

Section 3 -Information Access

3.0 Information Access

(a) Public Information

This information includes:

- Public record filings with regulatory agencies. (Some examples include, but are not limited to, ISO Budget Data required for ISO Tariff Filings; and data associated with the Open Access Transmission Tariff.)

- Data posted on the Open Access Same-Time Information System ("OASIS"). (Some examples include, but are not limited to, Transmission Facilities Information including System Inventory; New Applications; Scheduling Information, Real Time Tie Line Use and Surplus Availability; Aggregate MW of generation operating out of merit (for transmission, reliability, and VAR) by Reliability Region (these Regions will be defined by the ISO, such that no *Confidential* or Strategic Information is released), Real Time Operating Reserve Availability and curtailment or interruption of External Transactions.)

- Information and/or reports that are required to be filed with the Federal Energy Regulatory Commission ("FERC") (unless specifically required to be filed on a confidential basis). (For example, the Filed Documents.)

- Public Generator Information including System Inventory and New Applications. (Some examples include, but are not limited to, Capacity, Energy, Loads & Transmission (CELT) Report; and 18.4 Applications.)

- Public Market Information includes any items required to be made public by **(i)** the Filed Documents; **(ii)** other relevant documents, including without limitation the ISO New England Manuals and any other system rules, procedures or criteria for the operation of the New England system and administration of the Market and the Filed Documents; and **(iii)** the items listed in Aggregate Market Results, as posted under "Market Information" on the ISO website pursuant to this Information Policy. (Some examples include, but are not limited to, aggregate Market requirements and settlements; Clearing Prices; Locational Marginal Prices; lists of load zones, nodes and hubs; Emergency Energy notices; market monitoring input assumptions and threshold values; Financial Transmission Rights modeling and auction results; Auction Revenue Rights modeling and auction results; information relating to the Load Response Program; ICAP Market Schedules and UCAP auction results.)

- In addition, the System Operator shall publish each month's bid and offer information for all markets on its website on the first day of the fourth calendar month following the month during which the applicable demand bids and supply offers were in effect (e.g., bid and offer data for January would be released on May 1), provided that the information is presented in a manner that does not reveal the specific load or supply asset, its owners, or the name of the entity making the bid or offer, but that allows the tracking of each individual entity's bids and offers over time.

- Market test information including any information equivalent to Public Market Information derived from test programs for new markets or market software or simulations of proposed market improvement (includes any and all information necessary for evaluation of the impacts of a proposed new market or an improvement to an existing market, such as cost-shifting impacts and price impacts under certain conditions).

- Long-term system planning and operations information consisting of load forecasts, transmission models (including power flow, short circuit and stability models and their related base cases and contingency files), transfer limits used for planning purposes, Installed Capacity Requirements and Governance Participants and non-Governance Participants proposed generation. This information does not include near-term transmission models or transfer limits within New England that are

developed as part of system operations or real-time information from the control room energy management system; provided that, notwithstanding the provisions of Sections 3.0(b) and (g)(ii), the ISO may publish, on a weekly basis, the following information associated with NERC's alert regarding "Consideration of Actual Field Conditions in Determination of Facility Ratings" for each transmission facility affected by the alert: (i) the identification of the facility subject to a rating change; (ii) the original rating of the facility; (iii) the new rating of the facility which reflects the de-rating due to the NERC alert, and; (iv) the non-binding expected date that the transmission facility de-rating will be remediated.

- Public Reports required by the Filed Documents (including, but not limited to, evaluation of procedures for determination of Locational Marginal Prices as well as the awarding Financial Transmission Rights and associated Congestion Costs and Transmission Congestion Credits).

- Public Market Monitoring Information including, but not limited to, public reports by the Independent Market Advisor required by the Market Rules (includes the ISO's time and expenses in pursuing sanctionable behavior on a case-by-case basis and periodic reports of sanctions imposed and the sanctionable behavior upon which such sanctions were imposed, provided that the information is presented in a manner that does not allow for the identification of the Governance Participants by name or provide a manner for identifying such Governance Participants, except as otherwise provided in the Filed Documents).

- Any other information that is not *Confidential Information* that the ISO determines is appropriate for public dissemination because it will improve system reliability, the efficiency of the markets or public understanding of the New England system and the operations of the ISO.

This data may be made available to the public at large. (Fees may be applicable to cover process and handling expenses.) [This information corresponds to the MIS security rule "PB" Public.]

(b) Non-Public Transmission Information

This information includes:

- Information and/or reports that are filed with NERC. (Some examples include, but are not limited to, all NPCC data, see examples below.)

- Information and/or reports that are filed with the Northeast Power Coordinating Council (NPCC).

- Real-time system operations information, which is not posted on the OASIS, including but not limited to detailed operations data. (Some examples include, but are not limited to, real-time transmission line flows, real-time transfer limits, and real-time voltages.)

- Information relating to specific Generating facilities, which is required by transmission personnel to ensure the reliable operation of the New England bulk power system. (Some examples include, but are not limited to, detailed Generator operating characteristics; and dynamic swing recorder plots.)

- Transmission Operating Guides. (Some examples include, but are not limited to, guides for operation of Special Protection Systems; and transmission operations related to Stability Limits.)

- Information related to system restoration efforts. (Some examples include, but are not limited to, ISO and Governance Participants' detailed Power System Restoration Plans.)

This information may be made available to Reliability Councils and all Governance Participants' Transmission Personnel. The release of relevant transmission outage information to affected generators, to the extent required or desired for coordination of transmission and generation outages, shall be governed by the processes available for such coordination (OP3 or any successor or similar document), by the Codes of Conduct and by other applicable FERC regulation. There is no direct correlation to the MIS Security Rules and there is currently no specific transmission information distributed via the MIS.

(c) Governance Participant Specific Data

This information includes:

- Data not yet posted on the OASIS. (Some examples include, but are not limited to, Interface Transmission Service Schedules Lists.)

- *Confidential Information*, as defined in Section 2.1 of this Policy, for which this Governance participant, or an Agent thereof, has the right to receive the data. (Some examples include, but are not limited to, Product Obligation; and Load.)

- Invoice and Settlement Data. (Some examples include, but are not limited to, Governance Participant Phase I/II Hourly Transfer Capability Allocations; Electrical Load, Adjusted Net Interchange, Obligation, Entitlement, Charges, and Payments for each market.)

[This data may be made available to active users or agents of the specified Governance Participant. This information corresponds to the MIS security rule "SM" Settlement Rule.]

(d) Asset Specific Information – Near Real-Time

This information includes:

- Near real-time information related to the particular asset. (Some examples include, but are not limited to, Generation Levels (MW); Designations (MW); Automatic Generation Control Status, Operating Limits, Response Rates, unit forecast and operation information, and Real Time Status of External Contract Sales and/or Purchases for which a Governance Participant has a contract on file with the ISO.)

This data may be made available to those Governance Participants, or Agents thereof, who are joint Owners and/or Entitlement Holders in the Asset. [This information corresponds to the MIS security rules "OS" Ownership Rule, "RS" Responsible Party Rule and an Entitlement Holder Rule, currently not identified in the MIS security rules. As applicable, this data may also be made available to a Governance Participant who is a contractual party to external or internal bilateral contracts for the specified Asset, which corresponds to the MIS security rule "TH" Transaction Holder Rule.] The release of relevant generation outage information to affected transmission owners, to the extent required or desired for coordination of transmission and generation outages, shall be governed by the processes available for such coordination (OP3 or any successor or similar document), by the Codes of Conduct and by other applicable FERC regulation.

(e) Asset Specific Information – Forecast and post-Settlement

This information includes:

- Unit Forecast information relating to a particular Asset, which is necessary to determine the projected operation of particular Generators. (Some examples include, but are not limited to, Start Time; Generation; and Shut-Down Time.)

- Information relating to a particular Asset, which is necessary to determine the accuracy of Settlement. (Some examples include, but are not limited to, High Operating Limit; Generation; Ownership Share; and Duration on Automatic Generation Control.)

- Governance Participant input data. (Some examples include, but are not limited to, generation input data; and records of deficient performance.)

- Capability Responsibility (CR) data and calculations, for those specific Generating facilities for which a Governance Participant(s) has an ownership interest. (Some examples include, but are not limited to, Unit Capability Demonstrations and Audits; and Seasonal Claimed Capability.)

- All information, with the exception of bids, offers and meter data, necessary to verify Settlement data. (Some examples include, but are not limited to, Response Rate data; and Minimum Run-Time data.)

This data may be made available to those Governance Participants, or Agents thereof, who are joint Owners and/or Entitlement Holders in the Asset. [This information corresponds to the MIS security rules "OS" Ownership Rule, "RS" Responsible Party Rule and an Entitlement Holder Rule, currently not identified in the MIS security rules.] The release of relevant generation outage information to affected transmission owners, to the extent required or desired for coordination of transmission and generation outages, shall be governed by the processes available for such coordination (OP3 or any successor or similar document), by the Codes of Conduct and by other applicable FERC regulation.

(f) Meter, Bid and Offer Data

This information includes:

- *Confidential Information* submitted as input to the Market System. Bid and offer data may be made available to any Governance Participant with a Generation Ownership Share, or Agent thereof, for a specified Asset. [This information corresponds to the MIS security rules "RS" Responsible Party Rule.]

- A minimum power value derived by the ISO from a resource's Economic Minimum Limit may be included in the transmission models that are treated as public information pursuant to Section 3.0(a).

- Meter data may be made available to the Assigned Meter Reader for a specified Asset. There is no direct correlation to the MIS Security Rules and there is currently no specific MIS distribution of meter data. However, meter data may be manually distributed to the Host Participant whose unmetered load is calculated based on said meter data.

(g) Reliability, Operations and Area Control Information

(i) Reliability-Related Information

This information includes:

- Real-Time operating data, including *Confidential Information*, that is used to assure the reliable operation of the interconnected bulk power system and/or that may be authorized or required to be shared pursuant to reliability standard, NERC or NPCC rule, or by Commission request, order or rule. (Some examples include, but are not limited to, transmission interface limits, transmission line flows, line or circuit breaker status, generation output or phasor measurement data.)

Real-time operating data that is used to assure reliable operation of the interconnected bulk power system is typically shared by the ISO with the Commission, NERC, NPCC, and any applicable "regional entity" (as defined in the Federal Power Act), or any reliability coordinator, balancing authority, transmission operator or equivalent entity.

(ii) External Control Center Information

This information includes:

- All System Operations or Planning Information that relates to the particular external Control Center. (Some examples include, but are not limited to, transmission interface transfers and limits within the external control center area; and Inter-Area Emergency Assistance available, used for Planning purposes, under OP-4 conditions.)

- Information that is required to assure the reliable operation of the interconnected bulk power system. (Some examples include, but are not limited to, all information deemed necessary in the event of OP 4 implementation; and, under non-OP-4 system conditions, information related to Inter-Area flow control.)

- Inter-area Transmission Operating Guides that relate to the particular external control area. (Some examples include, but are not limited to, PV-20 Cross Trip SPS – available to New York; and Phase I Runback SPS – available to Hydro Quebec.)

- Confidential Information (under signature of confidentiality agreements that provide rights to Governance Participants equivalent to those granted in this Information Policy to notice of and opportunity to defend against any release of their Confidential Information) and non-confidential information may be shared among Control Areas for the purposes of increasing markets coordination, including elimination of seams, increasing market efficiency and study purposes of the interconnected bulk power system. (Some examples include, but are not limited to, ISO operations and markets information, including market monitoring information, provided that market monitoring information shall only be shared with independent market operators or independent market monitors and only in connection with particular investigations affecting regional markets.)

There is no direct correlation to the MIS Security Rules and there is no specific MIS distribution of External Control Center Information. This information is not available to Governance Participants, a subset thereof, or the Public at large, but is typically communicated by the ISO Operations (Control Room/Forecast Office) or Planning Department directly to External Control Center personnel.

(iii) Internal (Satellites) Control Center Information

This information includes:

- All System Operations or Planning Information. (Some examples include, but are not limited to, detailed system models; and transmission element data as detailed on the NX-9 forms.)

- Information relating to specific Generating facilities that is needed to assure the reliable operation of the New England Control Area. (Some examples include, but are not limited to, Generator constraints, including the reason for such constraint; and detailed Generator unit commitment.)

- Transmission Operating Guides. (Some examples include, but are not limited to, guides for operation of Special Protection Systems; and transmission operations related to Stability Limits.)

- New England and Satellite System Restoration Plans. (Some examples include, but are not limited to, the ISO, Satellite and Governance Participants' detailed Power System Restoration Plans.)

There is no direct correlation to the MIS Security Rules and there is no specific MIS distribution of Internal (Satellite) Control Center Information. This information is not available to Governance Participants, a subset thereof, or the Public at large, but is typically communicated by the ISO Operations (Control Room/Forecast Office) directly to Satellite personnel.

(h) Load Response Provider Information

This information is asset-specific Confidential Information, including:

- Retail customer information;
- Customer data;
- Load profiles, and;
- Demand response information provided at the request of the Internal Market Monitor pursuant to Section III.A.17.

Information relating to retail customers, customer data and load profiles is subject to certain state law restrictions and is not available to Governance Participants, a subset thereof, or the Public at large, but is typically communicated by the ISO Operations (Control Room/Forecast Office) directly to Load Response Provider personnel.

(i) ISO New England Information

This information includes:

- Any Governance Participant or Asset specific information as requested by the ISO, which will be maintained in accordance with this Policy. (Some examples include, but are not limited to, all Governance Participant and Asset specific information, which is available to the ISO.)

- Any ISO Employment Information and ISO Administrative Information not specifically listed in other categories.

ISO personnel, Consultants, Counsel, and Board Members may have access to any information defined in the categories listed above. This information corresponds to the MIS security rule "ISO" ISO New England.

All *Confidential Information*, as defined in Section 2.1 of this Policy, will only be distributed in accordance with this Policy.

All other data, which is not specifically defined and is not *Confidential Information*, may be released at the discretion of the ISO in accordance with the procedures set forth in Sections 3.1, 3.2 and 3.3 hereto.

(j) Critical Energy Infrastructure Information ("CEII")

This information includes:

- Information designated by a Governance Participant or the ISO as CEII, which is defined by FERC as "specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: (1) relates details about the production, generation, transportation, transmission, or distribution of energy; (2) could be useful to a person in planning an attack on critical infrastructure; (3) is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552 (2000); and (4) does not simply give the general location of the critical infrastructure."

- Reports, summaries, compilations, analyses, notes or other information which contain such information.

Access to CEII shall be granted by the ISO in accordance with the CEII disclosure processes posted on its website and, in the event that the CEII also falls within a category of information (including *Confidential Information*) described herein, in accordance with this Information Policy. Governance Participants shall treat CEII as if it were *Confidential Information*, notwithstanding any other provision of this Information Policy, and additionally shall maintain CEII in a secure place.

3.1 Information Requests

(a) Requesting Entities

As used in this Section 3.1, the term "Requesting Entity" shall mean any entity (other than the FERC, or the Commodity Futures Trading Commission ("CFTC")), or an Authorized Person, as defined in Section 3.3 of this Information Policy) that requests information from the ISO.

(b) Public Information

If a Requesting Entity requests that the ISO publish Public Information (as defined in Section 3.0(a) of this Information Policy) that is not currently published by the ISO, the ISO may after consultation with

the Participants Committee or its designated subcommittee or working group defer or deny such request if the ISO determines that publication of such data is not feasible at the time of such request due to resource limitations, including, without limitation, available software.

(c) Non-Public Information

(i) A Requesting Entity that desires to make a formal request for information that is not Public Information from the ISO, the resolution of which request shall be appealable under Section 3.1(e)(v) of this Information Policy, shall submit a formal written request to the ISO in the manner set forth in Section 3.1(d) below (a "Formal Information Request") for such information.

(ii) Requests for information from Requesting Entities to the ISO other than Formal Information Requests need not be in writing.

(iii) Any request for information from the FERC, or the CFTC, or from an Authorized Person (as defined in Section 3.3 of this Information Policy) shall be addressed according to the procedures set forth in Section 3.2 and Section 3.3 of this Information Policy, as applicable.

(d) Form of Request; Tracking

(i) Any Formal Information Request shall be directed to the point of contact designated by the ISO to handle such requests (the "ISO Information Contact"). The ISO shall post contact information for the ISO Information Contact on the ISO website.

(ii) A Formal Information Request shall be in writing, which shall include electronic communications addressed to the ISO Information Contact, and shall: (a) describe with particularity the information sought; (b) provide a description of the purpose of the information request; (c) state the time period for which such information is requested; (d) specifically designate such request as a Formal Information Request and make reference to Section 3.1(d)(ii) of the Information Policy; and (e) provide contact information for the person to whom the response to such Formal Information Request is to be directed.

(iii) The ISO Information Contact shall track all Formal Information Requests and provide a report indicating the nature of each request and the response to such request to the Markets Committee on a monthly basis.

(e) Timing and Notice

(i) The ISO Information Contact normally shall notify all affected Furnishing Entities within five (5) business days after receiving a Formal Information Request.

(ii) The ISO Information Contact normally shall provide the Requesting Entity with a response (an "Initial Response") within fifteen (15) business days after receiving the Formal Information Request (the "Request Date"). The Initial Response shall indicate either (A) that the ISO has made a decision on the Formal Information Request in accordance with Section 3.1(f)(i) below, in which case it shall describe such decision, or (B) that the ISO was unable to reach a decision, and will be consulting with the Participants Committee in accordance with Section 3.1(f)(ii) below.

(iii) If the Initial Response indicates that the ISO is further consulting with the Participants Committee, the ISO Information Contact normally shall provide the Requesting Entity with a follow-up response (a "Follow-Up Response") the earlier of ten (10) business days after a recommendation by the Participants Committee as set forth in Section 3.1(f)(ii) below or sixty (60) days following the Request Date, which response shall indicate either (A) that the ISO has made a decision on the Formal Information Request in accordance with Section 3.1(f)(ii) below, in which case it shall describe such decision, or (B) that the ISO has failed to make a decision with respect to the Formal Information Request, in which case such request shall be deemed denied.

(iv) The ISO Information Contact shall provide the Furnishing Entity(ies) with copies of any Initial Response or Follow-Up Response provided in response to a Formal Information Request on the same day that such responses are provided to the Requesting Entity. In addition, the ISO Information Contact shall provide the Furnishing Entity(ies) with at least ten (10) business days prior written notice of any release of *Confidential Information* or Strategic Information relating to such Furnishing Entity (whether such release is on the ISO's own initiative, in response to a Formal Information Request, or otherwise), which written notice shall inform such Furnishing Entity(ies) of its right to dispute such release under Section 3.1(e)(v) of the Information Policy.

(v) The Requesting Entity shall have the right to appeal any Initial Response that contains a decision with respect to a Formal Information Request and any Follow-Up Response. Any

affected Furnishing Entity shall have the right to appeal any Initial Response or Follow-Up Response that contains a decision with respect to a Formal Information Request and any decision by the ISO to release *Confidential Information* or Strategic Information (whether such release is on the ISO's own initiative, in response to a Formal Information Request, or otherwise). The Participants Committee shall have the right to appeal any Initial Response that contains a decision with respect to a Formal Information Request. Notice of any appeal shall be provided contemporaneously to the Participants Committee and the ISO Information Contact.

(vi) Any appeal of the ISO's actions under this Section 3.1 with respect to a Formal Information Request shall be subject to binding arbitration with FERC's Alternative Dispute Resolution Service, as further described in 18 C.F.R. §§ 385.604, 385.605. The ISO and the disputing entity(ies) shall use reasonable efforts to insure that an arbitrator is selected and a hearing is scheduled within thirty (30) days of the ISO receiving notice of an appeal. Unless otherwise agreed by all parties, the duration of any arbitration hearing will be limited to one day. The arbitrator's decision shall be binding on the respective parties; provided, however, that any of the respective parties to the arbitrator's decision shall be entitled to appeal the arbitrator's decision directly to FERC.

(vii) Suitable forms of notice and/or communications pursuant to this subsection shall include, but not be limited to, electronic communications.

(f) Consideration of Requests

(i) After receiving a Formal Information Request, the ISO shall first determine whether (X) the information requested is information described in Sections (a) through (i) of Section 3.0 and (Y) the Requesting Entity is a member of a user group specifically entitled to receive such information pursuant to Sections (a) through (i) of Section 3.0. If the ISO determines that the Requesting Entity is not entitled to receive the requested information pursuant to Sections (a) through (i) of Section 3.0, the ISO shall then determine if the requested information is *Confidential Information* or Strategic Information. The ISO may consult with the Independent Market Advisor, NEPOOL Counsel, the Furnishing Entity(ies), and/or the Participants Committee (as provided in Section 3.1(d)) during the process of making this determination.

(A) If the ISO determines that the information is *Confidential Information*, the ISO Information Contact will refer the request to the Furnishing Entity(ies) and the ISO will

not release the requested information unless it is directed to do so by the Furnishing Entity(ies) or ordered to do so by a court or regulatory authority with jurisdiction over such matters. If the Furnishing Entity(ies) directs the ISO to release the requested information, the ISO will next determine whether the requested information is Strategic Information as set forth in Section 3.1(c)(i)(B) below. The Furnishing Entity(ies) shall bear any costs reasonably incurred by the ISO in opposing the issuance of such an order requiring disclosure of the Furnishing Entity(ies)' *Confidential Information.* Notwithstanding the foregoing, upon the request of a regulatory agency, other than FERC or its staff or the CFTC or its staff, having appropriate jurisdiction and subject to an appropriate confidentiality order entered under such agency's procedures sufficient to preserve the confidential nature of the information submitted, and with advance notice to the Furnishing Entity(ies), the ISO Information Contact may submit *Confidential Information* to such agency.

(B) If the information requested is Strategic Information, the ISO shall determine whether to release the requested information, in consultation with the Independent Market Advisor, NEPOOL Counsel and/or the Furnishing Entity(ies), as the ISO deems appropriate. If the ISO releases such information, it will do so by making the information public.

(C) If the information requested is neither *Confidential Information* nor Strategic Information, the ISO shall determine whether to release the requested information; provided that the Participants Committee, acting on the recommendation of an appropriate Stakeholder Committee, may request the ISO to release the requested information.

(ii) If, after consultation with the Independent Market Advisor, NEPOOL Counsel and/or the Furnishing Entity, as appropriate, the ISO cannot, in its good faith judgment, determine the classification status of requested information or otherwise believes that a Formal Information Request raises policy questions that should be determined by the Governance Participants, then the following procedure shall apply:

(A) The ISO shall refer the request to the Participants Committee with its recommendation for action.

(B) The Participants Committee, acting on recommendation of a subcommittee or working group, as appropriate, may approve of or suggest modifications to the recommendation of the ISO. If the Participants Committee approves the ISO's recommendation, or if the ISO accepts the Participants Committee's suggested modifications, the Participants Committee's decision shall determine the response to the Formal Information Request; provided, however, that, to the extent that the information requested is found to be *Confidential Information*, the ISO shall continue to maintain the confidentiality of such information in accordance with the terms of this Information Policy.

(g) Release of Information; Prioritization of Formal Information Requests

(i) The ISO shall reasonably attempt to comply with any Formal Information Request that has been granted within thirty (30) days of the Initial Response or Follow-Up Response informing the Requesting Entity that its request has been granted. The ISO may condition the release of any information to a Requesting Entity upon payment of the ISO's reasonable cost to identify and prepare such information.

(ii) If the ISO does not have the resources available to comply with all outstanding Formal Information Requests within the time provided in clause (i) above, the ISO will consult with the Participants Committee or its designated subcommittee or working group to determine how such Formal Information Requests should be prioritized.

(h) Definition of Strategic Information

For purposes of this Policy, Strategic Information means any information, except Public Information, that would affect a Governance Participant's bid or offer strategy in the New England electric markets including information affecting the offer price for or cost of operation of a resource, the capacity or availability of a resource, or any other offer parameter for a resource.

Strategic Information includes *Confidential Information* supplied by Governance Participants to the extent such information would affect a Governance Participant's bid or offer strategy such as, for example:

- All offer prices and parameters for particular resources including bid blocks and times.

- Cost information regarding operation of one or more resources if and to the extent supplied to the ISO.

- Information regarding fuel availability for thermal resources or impoundment levels for hydroelectric facilities.

- Information regarding transmission outages, not otherwise made public, for scheduled maintenance or otherwise that affects the availability of certain generating resources.

Strategic Information may also include information calculated or produced by the ISO such as:

- Aggregate prices and quantities offered that are derived through the unit commitment process.

- Information regarding which resources will run or have run during any particular market settlement period.

- Information derived through the unit commitment process or the market settlement system as to units that run out of merit.

- Information regarding the existence or location of certain short-term transmission constraints.

No Strategic Information that is *Confidential Information* will be released except in compliance with the provisions of this Information Policy regarding *Confidential Information.*

3.2 Disclosure to FERC and the CFTC

(a) Procedures for Disclosure to FERC

If the FERC or its staff, during the course of an investigation or otherwise, requests information from the ISO that is *Confidential Information* or CEII, the ISO shall provide the requested information to the FERC or its staff, within the time provided for in the request for information. In providing *Confidential Information* to FERC or its staff, the ISO shall, consistent with 18 C.F.R §§ 1b.20 and 388.112, request that the information be treated as confidential and non-public by the FERC and its staff and that the information be withheld from public disclosure. The ISO shall notify any affected Furnishing Entity(ies) (1) when it is notified by FERC or its staff, that a request for disclosure of *Confidential Information* has

been received at which time the ISO and the affected Furnishing Entity(ies) may respond before such information would be made public; and (2) when it is notified by FERC or its staff that a decision to disclose *Confidential Information* has been made, at which time the ISO and the affected Furnishing Entity(ies) may respond before such information would be made public. In providing CEII to FERC or its staff, the ISO shall, consistent with 18 CFR § 388.112, request that the information be treated as CEII by the FERC and its staff.

(b) Procedures for Disclosure to the CFTC

Furnishing Entity(ies) permits the ISO to provide *Confidential Information* or CEII to the CFTC or its staff in response to a subpoena or other request for information or documentation without notifying Furnishing Entity(ies) prior to providing such information to the CFTC. The ISO shall provide the requested information or documentation to the CFTC or its staff within the time provided for in the request for information or documentation. In providing *Confidential Information* or CEII to the CFTC or its staff, the ISO shall: (i) request, on behalf of the Furnishing Entity(ies), that the information be treated as confidential and non-public by the CFTC and its staff, as provided in 17 C.F.R. § 145.9; and (ii) make clear through the confidentiality legend required by 17 C.F.R. § 145.9 that both the ISO and the Furnishing Entity(ies) are the submitters of the *Confidential Information* or CEII as provided under 17 C.F.R. § 145.9.

3.3 Disclosure to Authorized Persons and ISO/MMU Requesting Entities

(a) Definitions

For purposes of this Section 3.3, the following terms shall have the meanings set forth below:

"Affected Governance Participant" shall mean a Governance Participant, which, as a result of its Participation in the markets administered by the ISO, provided Confidential Market Information to the ISO, which Confidential Market Information is requested by or is disclosed to an Authorized Person under a Non-Disclosure Agreement.

"Authorized Commission" shall mean a State public utility commission within the geographic limits of the New England Control Area that regulates the distribution or supply of electricity to retail customers and is legally charged with monitoring the operation of wholesale or retail markets serving retail suppliers or customers within its State.

"Authorized Person" shall mean a person who has executed a Non-Disclosure Agreement, and is authorized in writing by an Authorized Commission to receive and discuss Confidential Market Information. Authorized Persons may include attorneys representing an Authorized Commission, consultants and/or contractors directly employed by an Authorized Commission, provided; however, that consultants or contractors may not initiate requests for Confidential Market Information from the ISO or the IMMU.

"Confidential Market Information" shall mean *Confidential Information* consisting of market data relating to the markets administered by the ISO, including data supplied by Governance Participants and aggregate data regularly compiled by the ISO. Confidential Market Information shall not include the following categories of information without excluding any objective market data associated with them that would otherwise be provided under the first sentence of this definition: (i) draft versions of reports and analyses, (ii) internal ISO documents not related to market data, (iii) attorney-client communications, (iv) attorney work-product privileged information, (v) communications about Confidential Market Information between an Affected Governance Participant and the ISO/IMMU, except to the extent that the communications become part of final written reports or final written analyses by the ISO/IMMU, (vi) communications between an Affected Governance Participant and the ISO made on a confidential basis as part of a settlement proceeding or negotiation; and (vii) information provided to the ISO on a confidential basis as part of an Alternative Dispute Resolution proceeding.

"Information Request" shall mean a written request, in accordance with the terms of this Section 3.3 for disclosure of Confidential Market Information pursuant to Section 3.3 of this Information Policy.

"ISO/MMU Requesting Entity" shall mean an independent system operator or regional transmission organization subject to the Commission's jurisdiction, or its market monitor, that is requesting Confidential Market Information pursuant to Section 3.3(c) of this Information Policy.

"Non-Disclosure Agreement" shall mean an agreement between an Authorized Person and the ISO pursuant to Section 3.3 of this Information Policy, the form of which is appended to this Information Policy (Appendix A), wherein the Authorized Person is given access to otherwise restricted Confidential Market Information, for the benefit of their respective Authorized Commission.

"State Certification" shall mean the Certification of an Authorized Commission, pursuant to Section 3.3 of this Information Policy, the form of which is appended to this Information Policy (Appendix B),

wherein the Authorized Commission identifies all Authorized Persons employed or retained by such Authorized Commission, a copy of which shall be filed with FERC.

"Third Party Request" shall mean any request or demand by any entity upon an Authorized Person, an Authorized Commission or an ISO/MMU Requesting Entity for release or disclosure of Confidential Market Information provided to the Authorized Person, Authorized Commission or ISO/MMU Requesting Entity by the ISO, the Internal Market Monitor or the External Market Monitor. A Third Party Request shall include, but shall not be limited to, any subpoena, discovery request, or other request for Confidential Market Information made by any: (i) federal, state, or local governmental subdivision, department, official, agency or court, or (ii) arbitration panel, business, company, entity or individual.

(b) Procedures for Disclosures to Authorized Persons

(i) Notwithstanding anything in this section to the contrary, the ISO and/or the External Market Monitor shall disclose Confidential Market Information, otherwise required to be maintained in confidence pursuant to this Information Policy, to an Authorized Person under the following conditions:

(1) The Authorized Person has executed a Non-Disclosure Agreement with the ISO representing and warranting that he or she: (i) is an Authorized Person; (ii) is duly authorized to enter into and perform the obligations of the Non-Disclosure Agreement; (iii) has adequate procedures to protect against the release of any Confidential Market Information received, (iv) is familiar with, and will comply with any applicable procedures of the Authorized Commission which the Authorized Person represents, (v) covenants and agrees on behalf of himself or herself not to disclose the Confidential Market Information and to deny any Third Party Requests and defend against any legal process which seeks the release of any Confidential Market Information received in contravention of the terms of the Non-Disclosure Agreement, and (vi) is not in breach of any Non-Disclosure Agreement entered into with the ISO.

(2) The Authorized Commission employing or retaining the Authorized Person has provided the ISO with: (a) a final order of FERC prohibiting the release by the Authorized Person or the Authorized Commission of Confidential Market Information in accordance with the terms of this Information Policy and the Non-Disclosure Agreement; and (b) either an order of such Authorized Commission or a certification from counsel to

such Authorized Commission, confirming that the Authorized Commission (i) has statutory authority to protect the confidentiality of any Confidential Market Information received from public release or disclosure and from release or disclosure to any other entity, (ii) will defend against any disclosure of Confidential Market Information pursuant to any Third Party Request through all available legal process, including, but not limited to, obtaining any necessary protective orders, (iii) will provide the ISO with prompt notice of any such Third Party Request or legal proceedings and will consult with the ISO and/or any Affected Governance Participant in its efforts to deny the Third Party Request or defend against such legal process, (iv) in the event a protective order or other remedy is denied, will direct Authorized Persons authorized by it to furnish only that portion of the Confidential Market Information which their legal counsel advises the ISO in writing is legally required to be furnished, (v) will exercise its best efforts to obtain assurance that confidential treatment will be accorded to such Confidential Market Information and (vi) has adequate procedures to protect against the release of such Confidential Market Information; and (c) confirmation in writing that the Authorized Person is authorized by the Commission to enter into the Non-Disclosure Agreement and to receive Confidential Market Information under this Information Policy.

(3) The Authorized Commission employing or retaining the Authorized Person has provided the ISO with a State Certification.

(4) The ISO and the External Market Monitor shall be expressly entitled to rely upon such FERC and Authorized Commission orders, the State Certification and/or certifications of counsel in providing Confidential Market Information to the Authorized Person, and shall in no event be liable, or subject to damages or claims of any kind or nature hereunder due to the ineffectiveness of the FERC and/or Commission orders, or the inaccuracy of such certification of counsel.

(5) The Authorized Person may discuss Confidential Market Information with other Authorized Persons who are parties to Non-Disclosure Agreements, provided; however, that the ISO shall have confirmed in advance and in writing that it has previously released the Confidential Market Information in question to such Authorized Persons. The ISO shall respond to any written request for confirmation within two (2) business days of its receipt.

(6) The ISO shall maintain a schedule of all Authorized Persons and the Authorized Commissions they represent, which shall be made publicly available on the ISO's website or by written request. Such schedule shall be compiled by the ISO, based on information provided by any Authorized Person and/or Authorized Commission. The ISO shall update the schedule promptly upon receipt of information from an Authorized Person or Authorized Commission, but shall have no obligation to verify or corroborate any such information, and shall not be liable or otherwise responsible for any inaccuracies in the schedule due to incomplete or erroneous information conveyed to and relied upon by the ISO in the compilation and/or maintenance of the schedule.

(ii) The External Market Monitor or other designated representative of the ISO may, in the course of discussions with any Authorized Person, orally disclose information otherwise required to be maintained in confidence, without the need for a prior Information Request. Such oral disclosures shall provide enough information to enable the Authorized Person or their Authorized Commission to determine whether additional Information Requests for information are appropriate. The External Market Monitor or other representative of the ISO will not make any written or electronic disclosures of Confidential Market Information to the Authorized Person pursuant to this section. In any such discussions, the External Market Monitor or other representative of the ISO shall ensure that the individual or individuals receiving such Confidential Market Information are Authorized Persons as defined herein, request that the Authorized Person describe the purpose of the inquiry, orally designate Confidential Market Information that is disclosed, and refrain from identifying any specific Affected Governance Participant whose information is disclosed. The External Market Monitor or other representative of the ISO shall also be authorized to assist Authorized Persons in interpreting Confidential Market Information that is disclosed. The External Market Monitor or representative of the ISO shall provide any Affected Governance Participant and counsel for the Participants Committee with oral notice of any oral disclosure immediately, but not later than one (1) business day after the oral disclosure. Such oral notice to the Affected Governance Participant shall include the substance of the oral disclosure, but shall not reveal any Confidential Market Information of any other Governance Participant and must be received by the Affected Governance Participant before the name of the Affected Governance Participant is released to the Authorized Person, provided; however, the identity of the Affected Party must be made to the Authorized Person within two (2) business days of the initial oral disclosure. The ISO shall provide an Affected

Governance Participant and counsel for the Participants Committee with written notice, which shall include electronic communication, of any oral disclosure as soon as possible, but not later than two (2) business days after the date of the oral disclosure.

(iii) As regards Information Requests:

(1) Information Requests to the ISO shall be in writing, which shall include electronic communications addressed to the External Market Monitor or other designated representative of the ISO, and shall: (a) describe with particularity the information sought; (b) provide a description of the purpose of the Information Request; (c) state the time period for which Confidential Market Information is requested; and (d) re-affirm that only the Authorized Person shall have access to the Confidential Market Information requested. The ISO shall provide an Affected Governance Participant and counsel for the Participants Committee with written notice, which shall include electronic communication, of an Information Request of the Authorized Person as soon as possible, but not later than two (2) business days after the receipt of the Information Request.

(2) Subject to the provisions of section (iii)(3), the ISO shall supply Confidential Market Information to the Authorized Person in response to any Information Request within five (5) business days of the receipt of the Information Request, to the extent that the requested Confidential Market Information can be made available within such period, provided; however, that in no event shall Confidential Market Information be released prior to the end of the fourth (4th) business day without the express consent of the Affected Governance Participant. To the extent that the ISO cannot reasonably prepare and deliver the requested Confidential Market Information within such five (5) day period, it shall, within such period, provide the Authorized Person with a written schedule for the provision of such remaining Confidential Market Information. Upon providing Confidential Market Information to the Authorized Person, the ISO shall either provide a copy of the Confidential Market Information to the Affected Governance Participant(s), or provide a listing of the Confidential Market Information disclosed, provided; however, that the ISO shall not reveal any Governance Participant's Confidential Market Information to any other Governance Participant.

(3) Notwithstanding section (iii)(2), above, should the ISO, an Affected Governance Participant, or the Participants Committee (with respect to an Information Request that applies to multiple Governance Participants) object to an Information Request or any portion thereof, any of them may, within four (4) business days following the ISO's receipt of the Information Request, request, in writing, a conference with the Authorized Commission or the Authorized Commission's authorized designee to resolve differences concerning the scope or timing of the Information Request, provided; however, nothing herein shall require the Authorized Commission to participate in any conference. Any party to the conference may seek assistance from FERC staff in resolution of the dispute. Should such conference be refused by any participant, or not resolve the dispute, then the ISO, the Affected Governance Participant, the Participants Committee (with respect to an Information Request that applies to multiple Governance Participants) or the Authorized Commission may initiate appropriate legal action at FERC within three (3) business days following receipt of written notice from any conference participant terminating such conference. Any complaints filed at FERC objecting to a particular Information Request shall be designated by the party as a "fast track" complaint and each party shall bear its own costs in connection with such FERC proceeding. If no FERC proceeding regarding the Information Request is commenced within such three day period, the ISO shall utilize its best efforts to respond to the Information Request promptly. During any pending FERC proceeding regarding an Information Request, the ISO shall continue to maintain the confidentiality of the Confidential Market Information subject to such Information Request.

(iv) In the event of any breach of a Non-Disclosure Agreement:

(1) The Authorized Person and/or their respective Authorized Commission shall promptly notify the ISO, who shall, in turn, promptly notify any Affected Governance Participant and counsel for the Participants Committee of any inadvertent or intentional release, or possible release, of Confidential Market Information provided pursuant to any Non-Disclosure Agreement.

(2) The ISO shall terminate such Non-Disclosure Agreement upon written notice to the Authorized Person and his or her Authorized Commission, and all rights of the Authorized Person thereunder shall thereupon terminate, provided; however, that the ISO

may restore an individual's status as an Authorized Person after consulting with the Affected Governance Participant and to the extent that: (i) the ISO determines that the disclosure was not due to the intentional, reckless or negligent action or omission of the Authorized Person; (ii) there were no harm or damage suffered by the Affected Governance Participant; or (iii) similar good cause shown. Any appeal of the ISO's actions under this section shall be to FERC.

(3) The ISO, the Affected Governance Participant, and/or the Participants Committee shall have the right to seek and obtain at least the following types of relief: (a) an order from FERC requiring any breach to cease and preventing any future breaches; (b) temporary, preliminary, and/or permanent injunctive relief with respect to any breach; and (c) the immediate return of all Confidential Market Information to the ISO.

(4) No Authorized Person shall have responsibility or liability whatsoever under the Non-Disclosure Agreement or this Information Policy for any and all liabilities, losses, damages, demands, fines, monetary judgments, penalties, costs and expenses caused by, resulting from, or arising out of or in connection with the release of Confidential Market Information to persons not authorized to receive it, provided that such Authorized Person is an employee or member of an Authorized Commission at the time of such unauthorized release. Nothing in this section (iv)(4) is intended to limit the liability of any person who is not an employee of or a member of an Authorized Commission at the, time of such unauthorized release for any and all economic losses, damages, demands, fines, monetary judgments, penalties, costs and expenses caused by, resulting from, or arising out of or in connection with such unauthorized release.

(5) Any dispute or conflict requesting the relief in section (iv)(2) or (iv)(3)(a) above, shall be submitted to FERC for hearing and resolution. Any dispute or conflict requesting the relief in section (4)(3)(c) above may be submitted to FERC or any court of competent jurisdiction for hearing and resolution.

(c) Procedures for Disclosures to an ISO/MMU Requesting Entity

(i) Notwithstanding anything in this section to the contrary, the ISO, the Internal Market Monitor or the External Market Monitor shall disclose Confidential Market Information,

otherwise required to be maintained in confidence pursuant to this Information Policy, to an ISO/MMU Requesting Entity under the following conditions:

(1) The ISO/MMU Requesting Entity has submitted to the ISO a written request for the disclosure of Confidential Market Information.

(2) The written request explains why the requested Confidential Market Information is necessary to an investigation that the ISO/MMU Requesting Entity is undertaking pursuant to its tariff, other governing documents, or an applicable law or regulation to determine (a) if a Market Violation is occurring or has occurred, (b) if market power is being or has been exercised, or (c) if a market design flaw exists that affects either the New England markets or the markets administered by the ISO/MMU Requesting Entity.

(3) The written request either (x) demonstrates, by providing copies of the relevant documentation, that the ISO/MMU Requesting Entity's tariff or other governing document limits further disclosure of the Confidential Market Information in a manner that satisfies all of the requirements set forth in Section 3.3(c)(ii) below, or (y) is accompanied by a non-disclosure agreement, which has been executed by both the ISO/MMU Requesting Entity and the ISO, that incorporates all of the requirements in Section 3.3(c)(ii) below, and a written certification that the ISO/MMU Requesting Entity possesses the legal authority to enter into the non-disclosure agreement, to be bound by it, and to perform all of the obligations of the non-disclosure agreement.

(4) If the ISO/MMU Requesting Entity is an independent system operator or regional transmission organization that meets the conditions in this Section 3.3(c), then the ISO shall also disclose the requested Confidential Market Information to the ISO/MMU Requesting Entity's market monitor, on condition that the receiving market monitor satisfy the confidentiality requirements and obligations specified in Section 3.3(c)(i)(3) above.

(ii) The ISO/MMU Requesting Entity's governing documents or non-disclosure agreement must:

(1) Covenant and agree not to disclose and to protect from disclosure the Confidential Market Information and to deny any Third Party Request and defend against any legal process which seeks the release of Confidential Market Information, except where disclosure is required by the Commission, by subpoena, or by other compulsory process;

(2) Represent and warrant that the ISO/MMU Requesting Entity has adequate procedures to protect against the release of Confidential Market Information;

(3) Establish a legally enforceable obligation to treat Confidential Market Information as confidential. Such obligation must be of a continuing nature, and must survive the rescission, termination or expiration of the tariff, other governing document or non-disclosure agreement;

(4) Require that the ISO/MMU Requesting Entity use the Confidential Market Information solely for the purpose of investigating (a) if a Market Violation is occurring or has occurred, (b) if market power is being or has been exercised, or (c) if a market design flaw exists that affects either the New England markets or the markets administered by the ISO/MMU Requesting Entity;

(5) Require state commissions to request Confidential Market Information directly from the ISO or the Internal Market Monitor, in a manner consistent with Section 3.3(b) of this Information Policy, and promptly inform the ISO or the Internal Market Monitor of any request received from a state commission for Confidential Market Information;

(6) Require the ISO/MMU Requesting Entity (a) to defend against any disclosure of Confidential Market Information pursuant to any Third Party Request through all available legal process, including, but not limited to, obtaining any necessary protective orders; (b) to provide the ISO, the Internal Market Monitor or the External

Market Monitor with prompt notice of any such Third Party Request or legal proceedings, and consult with the ISO, the Internal Market Monitor or the External Market Monitor in its efforts to deny the request or defend against such legal process; (c) in the event a protective order or other remedy is denied, to furnish only that portion of the Confidential Market Information which its legal counsel advises the ISO, the Internal Market Monitor or the External Market Monitor in writing is legally required to be furnished, and to exercise its best efforts to obtain assurance that confidential treatment will be accorded to such Confidential Market Information;

(7) Require the ISO/MMU Requesting Entity to promptly notify the ISO, the Internal Market Monitor or the External Market Monitor of any Third Party Requests for additional disclosure of the Confidential Market Information where Confidential Market Information has been disclosed to a court or regulatory body in response to a subpoena or other compulsory process, and to seek appropriate relief to prevent or limit further disclosure;

(8) Require destruction of the Confidential Market Information at the earlier of (a) five business days after a request from the ISO, the Internal Market Monitor or the External Market Monitor for the return of the Confidential Market Information is received, or (b) the conclusion or resolution of the investigation.

3.4 Disclosure to Academic Institutions

Notwithstanding anything to the contrary set forth herein, the ISO may disclose Confidential Market Information (as defined in Section 3.3), otherwise to be maintained in confidence pursuant to this Information Policy, to a research university (an "Authorized Institution"), solely for the purpose of academic research by Authorized Researchers (as defined below), under the following conditions:

(a) The Authorized Institution has delivered an information request to the ISO in writing (the "Academic Institution Information Request"), which shall include electronic communications addressed to the External Market Monitor, and shall: (i) describe with particularity the information sought; (ii) provide a description of the purpose of the Academic Institution Information Request ("Proposed Research"); (iii) state the time period for which the Confidential Market Information is requested; (iv) specify the individuals that will have access to such Confidential Market Information (the "Authorized Researchers") and (v) specify the source of

funding for the research to be performed with respect to the requested Confidential Market Information.

(b) The ISO shall review the merits of the Academic Institution Information Request and may, in its sole discretion, reject such request without providing notice to affected Governance Participants and the Participants Committee as required in subsection 3.4(c) below.

(c) In the event that the ISO does not initially reject the Academic Institution Information Request pursuant to subsection 3.4(b) above, the ISO shall provide affected Governance Participants and counsel to the Participants Committee with written notice, which shall include electronic communication, of an Academic Institution Information Request as soon as possible, but no later than five (5) business days after receipt of the Academic Institution Information Request. Such notice shall include all of the information contained in the Academic Institution Information Request.

(d) An authorized representative of the Authorized Institution has executed a non-disclosure agreement in the form attached hereto as Appendix C (the "Academic Institution Non-Disclosure Agreement") in which the Authorized Institution (i) represents and warrants that the Authorized Institution (w) will only share the Confidential Market Information with Authorized Researchers identified in the Academic Institution Information Request, solely to be used for the purpose of the Proposed Research; (x) is duly authorized to enter into and perform the obligations of the Academic Institution Non-Disclosure Agreement; (y) has adequate procedures to protect against the release of any Confidential Market Information received; and (z) is not in breach of any other Academic Institution Non-Disclosure Agreement entered into with the ISO; and (ii) covenants and agrees not to disclose the Confidential Market Information and to deny any third-party requests for the Confidential Market Information and defend against any legal process that seeks the release of any Confidential Market Information.

(e) The ISO shall provide affected Governance Participants and counsel to the Participants Committee written notice, which shall include electronic communication, of its determination whether to release Confidential Market Information in response to an Academic Institution Information Request as soon as possible, but no later than five (5) business days following the provision of the notice required in subsection (c) above. Notice of the ISO's determination shall also include all of the information contained in the Academic Institution Information Request,

and shall inform the affected Governance Participants of their right to object to such release, as well as the deadline for any such objection and shall specifically state that in the event that the affected Governance Participants do not object to such release, any information released by the ISO pursuant to an Academic Institution Information Request may be subject to publication by the Authorized Institution; provided that such publication may only be made (x) upon written consent of the ISO and (y) if any material the Authorized Institution proposes to publish, which is related to or that relies upon the Confidential Market Information, is sufficiently redacted or summarized in a manner so that it may not be identified. The ISO shall not release Confidential Market Information relating to any affected Governance Participant that objects to such release within ten (10) business days of the ISO's notice of its determination. Following the tenth (10th) business day after providing such notice, the ISO may, in its sole discretion, release Confidential Market Information relating to those affected Governance Participants that have not objected to such release to the Authorized Institution, provided, however, that the ISO shall redact all Confidential Market Information relating to any objecting affected Governance Participants, as applicable.

(f) In the event that an Authorized Institution or any Authorized Researcher publishes any material related to or that relies upon the Confidential Market Information, upon written consent of the ISO in accordance with Section 2.3.4 of the Academic Institution Non-Disclosure Agreement, the ISO shall provide notice to the Participants Committee regarding the medium (e.g., journal) in which the publication has been made.

APPENDIX A
FORM OF NON-DISCLOSURE AGREEMENT

THIS NON-DISCLOSURE AGREEMENT (the "Agreement") is made this _____ day of _____, 2004, by and between _____, an Authorized Person, as defined below, of _____ (the "State Commission") having jurisdiction within the State of _____, with offices at _____ and ISO New England Inc., a Delaware corporation, with offices at One Sullivan Road, Holyoke, Massachusetts, 01040-2841 ("ISO"). The State Commission and ISO shall be referred to herein individually as a "Party," or collectively as the "Parties."

RECITALS

Whereas, ISO serves as the Regional Transmission Organization for the New England Control Area, and operates and oversees wholesale markets for electricity pursuant to the requirements of the ISO Tariff, as defined below; and

Whereas, the External Market Monitor (as defined below) serves as the independent market monitor for ISO's wholesale markets for electricity, and

Whereas, the ISO New England Information Policy requires that ISO and the External Market Monitor maintain the confidentiality of Confidential Market Information; and

Whereas, the ISO New England Information Policy requires ISO and the External Market Monitor to disclose Confidential Market Information to Authorized Persons upon satisfaction of conditions stated in the ISO New England Information Policy, including, but not limited to, the execution of this Agreement by the Authorized Person and the maintenance of the confidentiality of such information pursuant to the terms of this Agreement; and

Whereas, ISO desires to provide Authorized Persons with the broadest possible access to Confidential Market Information, consistent with ISO's and the External Market Monitor's obligations and duties under the ISO New England Information Policy, the ISO Tariff and other applicable FERC directives; and

Whereas, this Agreement is a statement of the conditions and requirements, consistent with the requirements of the ISO New England Information Policy, whereby ISO and the External Market Monitor may provide Confidential Market Information to the Authorized Person.

NOW, THEREFORE, intending to be legally bound, the Parties hereby agree as follows:

1. Definitions

1.1 Affected Governance Participant. A Governance Participant, which as a result of its participation in the markets administered by ISO, provided Confidential Market Information to ISO, which Confidential Market Information is requested by, or is disclosed to an Authorized Person under this Agreement.

1.2 Authorized Commission. A State public utility commission within the geographic limits of the New England Control Area (as that term in defined in the ISO Tariff) that regulates the distribution or supply of electricity to retail customers and is legally charged with monitoring the operation of wholesale or retail markets serving retail suppliers or customers within its State.

1.3 Authorized Person. A person , including the undersigned, which has executed this Agreement and that is authorized in writing by an Authorized Commission to receive and discuss Confidential Market Information. Authorized Persons may include attorneys representing an Authorized Commission, consultants and/or contractors directly employed or retained by an Authorized Commission, provided however that consultants or contractors may not initiate requests for Confidential Market Information from ISO or the External Market Monitor.

1.4 Confidential Market Information. Shall mean *Confidential Information* (as defined in the ISO New England Information Policy) consisting of market data relating to the markets administered by ISO, including data supplied by Governance Participants and aggregate data regularly compiled by ISO. Confidential Market Information shall not include the following categories of information without excluding any objective market data associated with them that would otherwise be provided under the first sentence of this definition: (i) draft versions of reports and analyses, (ii) internal ISO documents not related to market data, (iii) attorney-client communications, (iv) attorney work-product privileged information, (v) communications about Confidential Market Information between an Affected Governance Participant and the ISO/External Market Monitor, except to the extent that the communications become part of final written reports or final written analyses by the ISO/External Market Monitor, (vi) communications between an Affected Governance Participant and ISO made on a confidential basis as part of a settlement proceeding or negotiation; and (vii) information provided to ISO on a confidential basis as part of an Alternative Dispute Resolution proceeding.

1.5 External Market Monitor. Shall have the meaning set forth in the ISO Tariff.

1.6 FERC. The Federal Energy Regulatory Commission.

1.7 Governance Participant. Shall have the meaning set forth in the ISO Tariff.

1.8 ISO New England Information Policy. Shall have the meaning set forth in the ISO Tariff.

1.9 Information Request. A written request, in accordance with the terms of this Agreement for disclosure of Confidential Market Information pursuant to Section 3.3 of the ISO New England Information Policy.

1.10 ISO Tariff. ISO's Transmission, Markets and Services Tariff, as it may be amended from time to time.

1.11 Third Party Request. Any request or demand by any entity upon an Authorized Person or an Authorized Commission for release or disclosure of Confidential Market Information. A Third Party Request shall include, but shall not be limited to, any subpoena, discovery request, or other request for Confidential Market Information made by any: (i) federal, state, or local governmental subdivision, department, official, agency or court, or (ii) arbitration panel, business, company, entity or individual.

2. Protection of Confidentiality.

2.1 Duty to Not Disclose. The Authorized Person represents and warrants that he or she: (i) is presently an Authorized Person as defined herein; (ii) is duly authorized to enter into and perform this Agreement; (iii) has adequate procedures to protect against the release of Confidential Market Information, and (iv) is familiar with, and will comply with, all such applicable State Commission procedures. The Authorized Person hereby covenants and agrees on behalf of himself or herself not to disclose the Confidential Market Information and to deny any Third Party Request and defend against any legal process which seeks the release of Confidential Market Information in contravention of the terms of this Agreement.

2.2 Conditions Precedent. As a condition of the execution, delivery and effectiveness of this Agreement by ISO and the continued provision of Confidential Market Information pursuant to the terms of this Agreement, the Authorized Commission shall, prior to the initial oral or written request for Confidential Market Information by an Authorized Person on its behalf, provide ISO with: (a) a final order of FERC prohibiting the release by the Authorized Person or the State Commission of Confidential Market Information in accordance with the terms of the Operating Agreement and this Agreement; and (b) either an order of the State Commission or a certification from counsel to the State Commission, confirming that the State Commission has statutory authority to protect the confidentiality of the Confidential Market Information from public release or disclosure and from release or disclosure to any other entity, and that it has adequate procedures to protect against the release of Confidential Market

Information; and (c) confirmation in writing that the Authorized Person is authorized by the State Commission to enter into this Agreement and to receive Confidential Market Information under the ISO New England Information Policy.

2.3 Discussion of Confidential Market Information with other Authorized Persons. The Authorized Person may discuss Confidential Market Information with other Authorized Persons who have executed non-disclosure agreements with ISO containing the same terms and conditions as this Agreement; provided, however, that ISO shall have confirmed in advance and in writing that ISO has previously released the Confidential Market Information in question to such Authorized Persons. ISO shall respond to any written request for confirmation within two (2) business days of its receipt.

2.4 Defense Against Third Party Requests. The Authorized Person shall defend against any disclosure of Confidential Market Information pursuant to any Third Party Request through all available legal process, including, but not limited to, obtaining any necessary protective orders. The Authorized Person shall provide ISO, and ISO shall provide each Affected Governance Participant and counsel for the Participants Committee, with prompt notice of any such Third Party Request or legal proceedings, and shall consult with ISO and/or any Affected Governance Participant in its efforts to deny the request or defend against such legal process. In the event a protective order or other remedy is denied, the Authorized Person agrees to furnish only that portion of the Confidential Market Information which their legal counsel advises ISO (and of which ISO shall, in turn, advise any Affected Governance Participants) in writing is legally required to be furnished, and to exercise their best efforts to obtain assurance that confidential treatment will be accorded to such Confidential Market Information.

2.5 Care and Use of Confidential Market Information.

2.5.1 Control of Confidential Market Information. The Authorized Person(s) shall be the custodian(s) of any and all Confidential Market Information received pursuant to the terms of this Agreement from ISO or the External Market Monitor.

2.5.2 Access to Confidential Market Information. The Authorized Person shall ensure that Confidential Market Information received by that Authorized Person is disseminated only to those persons publicly identified as Authorized Persons on Exhibit "A" to the certification provided by the State Commission pursuant to the procedures contained in Section 2.2 of this Agreement.

2.5.3 Schedule of Authorized Persons.

(i) The Authorized Person shall promptly notify ISO of any change that would affect the Authorized Person's status as an Authorized Person, and in such event shall request, in writing, deletion from the schedule referred to in section (ii), below.

(ii) ISO shall maintain a schedule of all Authorized Persons and the Authorized Commissions they represent, which shall be made publicly available on ISO's website and/or by written request. Such schedule shall be compiled by ISO, based on information provided by any Authorized Person and/or Authorized Commission. ISO shall update the schedule promptly upon receipt of information from an Authorized Person or Authorized Commission, but shall have no obligation to verify or corroborate any such information, and shall not be liable or otherwise responsible for any inaccuracies in the schedule due to incomplete or erroneous information conveyed to and relied upon by ISO in the compilation and/or maintenance of the schedule.

2.5.4 Use of Confidential Market Information. The Authorized Person and his or her Authorized Commission shall use the Confidential Market Information solely for the purpose of assisting the Authorized Commission in discharging its legal responsibility to monitor the wholesale and retail electricity markets, operations, transmission planning and siting, and generation planning and siting materially affecting retail customers within the State in which the Authorized Commission has regulatory jurisdiction, and for no other purpose. Without limiting the foregoing, the Authorized Person and his or her Authorized Commission shall not use its right to acquire Confidential Market Information as a means of conducting discovery or providing evidence during an adversarial proceeding against an Affected Governance Participant or any group of Participants. The Authorized Person and his or her Authorized Commission, however, shall not be prevented from using in an adversarial proceeding Confidential Market Information the Authorized Commission has obtained if: (i) such information becomes known in that proceeding through disclosure by entities other than the Authorized Commission; and (ii) the Authorized Commission discloses such Confidential Market Information consistent with the protections and procedures governing the disclosure of Confidential Market Information to parties in that proceeding; or (iii) the information being disclosed no longer meets the definition of Confidential Market Information.

2.5.5 Return of Confidential Market Information. Upon completion of the inquiry or investigation referred to in the Information Request, or for any reason the Authorized Person is, or will no longer be an Authorized Person, the Authorized Person shall (a) return the Confidential Market Information and all copies thereof to ISO, or (b) provide a certification that the Authorized Person has destroyed all paper

copies and deleted all electronic copies of the Confidential Market Information, unless such actions are inconsistent with or prohibited by applicable state law, in which case the Authorized Person shall continue to maintain the confidentiality of the Confidential Market Information in accordance with the terms and conditions of this Agreement. ISO may waive this condition in writing if such Confidential Market Information has become publicly available or non-confidential in the course of business or pursuant to the ISO Tariff or order of the FERC.

2.5.6 Notice of Disclosures. The Authorized Person, directly or through the Authorized Commission, shall promptly notify ISO, and ISO shall promptly notify any Affected Governance Participant, of any inadvertent or intentional release or possible release of the Confidential Market Information provided pursuant to this Agreement. The Authorized Person shall take all steps to minimize any further release of Confidential Market Information, and shall take reasonable steps to attempt to retrieve any Confidential Market Information that may have been released.

2.6 Ownership and Privilege. Nothing in this Agreement, or incident to the provision of Confidential Market Information to the Authorized Person pursuant to any Information Request, is intended, nor shall it be deemed, to be a waiver or abandonment of any legal privilege that may be asserted against, subsequent disclosure or discovery in any formal proceeding or investigation. Moreover, no transfer or creation of ownership rights in any intellectual property comprising Confidential Market Information is intended or shall be inferred by the disclosure of Confidential Market Information by ISO, and any and all intellectual property comprising Confidential Market Information disclosed and any derivations thereof shall continue to be the exclusive intellectual property of ISO and/or the Affected Governance Participant.

3. Procedure for Information Requests

3.1 Written Requests. Information Requests to ISO shall be in writing, which shall include electronic communications, addressed to the External Market Monitor or other ISO representatives as specified by ISO, with a concurrent copy to ISO's General Counsel, and shall: (a) describe with particularity the information sought; (b) provide a description of the purpose of the Information Request; (c) state the time period for which information is requested; and (d) re-affirm that only the Authorized Person shall have access to the Confidential Market Information requested. ISO shall provide an Affected Governance Participant and counsel for the Participants Committee with written notice, which shall

include electronic communication, of an Information Request of the Authorized Person as soon as possible, but not later than two (2) business days after the receipt of the Information Request.

3.2 Oral Disclosures by the External Market Monitor. The External Market Monitor or other ISO representatives as specified by ISO may, in the course of discussions with an Authorized Person, orally disclose information otherwise required to be maintained in confidence, without the need for a prior Information Request. Such oral disclosures shall provide enough information to enable the Authorized Person or the State Commission to determine whether additional Information Requests for information are appropriate. The External Market Monitor or other ISO representative will not make any written or electronic disclosures of Confidential Market Information to the Authorized Person pursuant to this section. In any such discussions, the External Market Monitor or other ISO representative shall ensure that the individual or individuals receiving such Confidential Market Information are Authorized Persons under this Agreement, request that the Authorized Person describe the purpose of the inquiry, orally designate Confidential Market Information that is disclosed and refrain from identifying any specific Affected Governance Participant whose information is disclosed. The External Market Monitor or other ISO representative shall also be authorized to assist Authorized Persons in interpreting Confidential Market Information that is disclosed. ISO or the External Market Monitor shall (i) maintain a written record of oral disclosures pursuant to this section, which shall include the date of each oral disclosure and the Confidential Market Information disclosed in each such oral disclosure, and (ii) provide any Affected Governance Participant and counsel for the Participants Committee with oral notice of any oral disclosure immediately, but not later than one (1) business day after the oral disclosure. Such oral notice to the Affected Governance Participant shall include the substance of the oral disclosure, but shall not reveal any Confidential Market Information of any other Governance Participant and must be received by the Affected Governance Participant before the name of the Affected Governance Participant is released to the Authorized Person; provided however, the identity of the Affected Party must be made available to the Authorized Person within two (2) business days of the initial oral disclosure. ISO shall provide an Affected Governance Participant and counsel for the Participants Committee with written notice, which shall include electronic communication, of any oral disclosure as soon as possible, but not later than two (2) business days after the date of the initial oral disclosure.

3.3 Response to Information Requests.

3.3.1 Subject to the provisions of Section 3.3.2 below, ISO shall supply Confidential Market Information to the Authorized Person in response to any Information Request within five (5) business

days of the receipt of the Information Request, to the extent that the requested Confidential Market Information can be made available within such period; provided however, that in no event shall Confidential Market Information be released prior to the end of the fourth (4th) business day without the express consent of the Affected Governance Participant. To the extent that ISO can not reasonably prepare and deliver the requested Confidential Market Information within such five (5) day period, ISO shall, within such period, provide the Authorized Person with a written schedule for the provision of such remaining Confidential Market Information. Upon providing Confidential Market Information to the Authorized Person, ISO shall either provide a copy of the Confidential Market Information to the Affected Governance Participant(s), or provide a listing of the Confidential Market Information disclosed; provided, however, that ISO shall not reveal any Governance Participant's Confidential Market Information to any other Governance Participant.

3.3.2 Notwithstanding section 3.3.1, above, should ISO or an Affected Governance Participant or the Participants Committee (with respect to an Information Request that applies to multiple Governance Participants) object to an Information Request or any portion thereof, ISO, the Affected Governance Participant and/or the Participants Committee may, within four (4) business days following ISO's receipt of the Information Request, request, in writing (which shall include electronic communication) addressed to the State Commission with a copy to either the Affected Governance Participant, ISO and/or counsel to the Participants Committee, as the case may be, a conference with the State Commission or the State Commission's authorized designee to resolve differences concerning the scope or timing of the Information Request; provided, however, nothing herein shall require the State Commission to participate in any conference. Any party to the conference may seek assistance from FERC staff in resolution of the dispute. Should such conference be refused by any participant, or not resolve the dispute, then ISO, the Affected Governance Participant, the Participants Committee (with respect to an Information Request that applies to multiple Governance Participants) or the State Commission may initiate appropriate legal action at FERC within three (3) business days following receipt of written notice from any conference participant terminating such conference. Any complaints filed at FERC objecting to a particular Information Request shall be designated by the party as a "fast track" complaint and each party shall bear its own costs in connection with such FERC proceeding. If no FERC proceeding regarding the Information Request is commenced by ISO, the Affected Governance Participant or the State Commission within such three day period, ISO shall utilize its best efforts to respond to the Information Request promptly. During any pending FERC proceeding regarding an Information Request, ISO shall continue to maintain the confidentiality of the Confidential Market Information subject to such Information Request.

3.3.3 To the extent that a response to any Information Request requires disclosure of Confidential Market Information of two or more Affected Governance Participants, ISO shall, to the extent possible, segregate such information and respond to the Information Request separately for each Affected Governance Participant.

4. Remedies.

4.1 Material Breach. The Authorized Person agrees that release of Confidential Market Information to persons not authorized to receive it constitutes a breach of this Agreement and may cause irreparable harm to ISO and/or the Affected Governance Participant. In the event of a breach of this Agreement by the Authorized Person, ISO shall terminate this Agreement upon written notice to the Authorized Person and his or her Authorized Commission, and all rights of the Authorized Person hereunder shall thereupon terminate; provided, however, that ISO may restore an individual's status as an Authorized Person after consulting with the Affected Governance Participant and to the extent that: (i) ISO determines that the disclosure was not due to the intentional, reckless or negligent action or omission of the Authorized Person; (ii) there were no harm or damages suffered by the Affected Governance Participant; or (iii) similar good cause shown. Any appeal of ISO's actions under this section shall be to FERC.

4.2 Judicial Recourse. In the event of any breach of this Agreement, ISO, the Affected Governance Participant and/or the Participants Committee shall have the right to seek and obtain at least the following types of relief: (a) an order from FERC requiring any breach to cease and preventing any future breaches; (b) temporary, preliminary, and/or permanent injunctive relief with respect to any breach; and (c) the immediate return of all Confidential Market Information to ISO. The Authorized Person expressly agrees that in the event of a breach of this Agreement, any relief sought properly includes, but shall not be limited to, the immediate return of all Confidential Market Information to ISO.

4.3 Waiver of Monetary Damages. No Authorized Person shall have responsibility or liability whatsoever under this Agreement for any and all liabilities, losses,
damages, demands, fines, monetary judgments, penalties, costs and expenses caused by, resulting from, or arising out of, or in connection with, the release of Confidential Market Information to persons not authorized to receive it, provided that such Authorized Person is an employee or Governance Participant of an Authorized Commission at the time of such unauthorized release. Nothing in this Section 4.3 is intended to limit the liability of any person who is not an employee of or a Governance Participant of an

Authorized Commission at the time of such unauthorized release for any and all economic losses, damages, demands, fines, monetary judgments, penalties, costs and expenses caused by, resulting from, or arising out of or in connection with such unauthorized release.

5. Jurisdiction. The Parties agree that (i) any dispute or conflict requesting the relief in sections 4.1 and 4.2(a) above shall be submitted to FERC for hearing and resolution; (ii) any dispute or conflict requesting the relief in section 4.2(c) above may be submitted to FERC or any court of competent jurisdiction for hearing and resolution; and (iii) jurisdiction over all other actions and requested relief shall lie in any court of competent jurisdiction.

6. Notices. All notices required pursuant to the terms of this Agreement shall be in writing, and served at the following addresses or email addresses:

If to the Authorized Person:

-

_____

—

_____

—

_____

—

(email address)

with a copy to

_____

—

_____

—

_____

—

(email address)

If to Counsel for the Participants Committee:

_____

—

_____

_____

_____

_

(email address)

with a copy to

_____

_

_____

_

_____

_

(email address)

If to ISO:

_____

_____

_____

(email address)

with a copy to

_____

_____

_____

(email address)

7. **Severability and Survival.** In the event any provision of this Agreement is determined to be unenforceable as a matter of law, the Parties intend that all other provisions of this Agreement remain in full force and effect in accordance with their terms. In the event of conflicts between the terms of this Agreement and the Operating Agreement, the terms of the Operating Agreement shall in all events be controlling. The Authorized Person acknowledges that any and all obligations of the Authorized Person hereunder shall survive the severance or termination of any employment or retention relationship between the Authorized Person and their respective Authorized Commission.

8. **Representations.** The undersigned represent and warrant that they are vested with all necessary corporate, statutory and/or regulatory authority to execute and deliver this Agreement, and to perform all of the obligations and duties contained herein.

9. Third Party Beneficiaries. The Parties specifically agree and acknowledge that each Governance Participant is an intended third party beneficiary of this Agreement entitled to enforce its provisions.

10. Counterparts. This Agreement may be executed in counterparts and all such counterparts together shall be deemed to constitute a single executed original.

11. Amendment. This Agreement may not be amended except by written agreement executed by authorized representatives of the Parties.

ISO NEW ENGLAND INC.	AUTHORIZED PERSON
By:	By:
_____	_____
Name:	Name:
Title:	Title:

APPENDIX B
FORM OF CERTIFICATION

This Certification (the "Certification") is given this _____ day of _____, 200_, by _____, a _____ (the "Authorized Commission"), to and for the benefit of ISO New England Inc. ("ISO") and its Governance Participants. The Authorized Commission and ISO shall be referred to herein collectively as the "Parties".

Whereas, the Authorized Commission has designated the individuals on attached Exhibit "A" (the "Authorized Persons") to receive Confidential Market Information from ISO, and

Whereas, the Authorized Persons and ISO have, or will, enter into non-disclosure agreements, governing the rights and obligations of the Authorized Persons, ISO and others regarding the Authorized Persons' access to, provision of, use and control of the Confidential Market Information (the "Non-Disclosure Agreements"), and

Whereas, as a condition precedent to the execution of the Non-Disclosure Agreements and provision of Confidential Market Information to the Authorized Persons, the Authorized Commission is required to make certain representations and warranties to ISO, and

Whereas, ISO agrees to provide Confidential Market Information to the Authorized Persons, in their capacity as agents of the Authorized Commission, subject to the terms of this Certification, the Non-Disclosure Agreements, and an appropriate order of the Federal Energy Regulatory Commission protecting the confidentiality of such data;

Whereas, the Parties desire to set forth those representations and warranties herein.

Now, therefore, the Authorized Commission hereby makes the following representations and warranties, all of which shall be true and correct as of the date of execution of this Certification, and at all times thereafter, and with the express understanding that ISO and any Affected Member shall rely on each representation and/or warranty:

1. **Definitions.** Terms contained, but not defined, herein shall have the definitions or meanings ascribed to such terms in the Non-Disclosure Agreement or the ISO New England Information Policy.

2. **Requisite Authority.**

a. The Authorized Commission hereby certifies that it has all necessary legal authority to execute, deliver, and perform the obligations in this Certification.

b. Each Authorized Person is, at the time of the execution of this Certification, an employee of, or consultant to, the Authorized Commission, and has not materially breached any existing or past nondisclosure agreement or obligation, except as has been disclosed by the Authorized Commission to ISO in writing.

c. The Authorized Persons have, through all necessary action of the Authorized Commission, been appointed and directed by the Authorized Commission to execute and deliver the Non-Disclosure Agreements to ISO and receive Confidential Market Information on the Authorized Commission's behalf and for its benefit.

d. The Authorized Commission will, at all times after the provision of Confidential Market Information to the Authorized Persons, provide ISO with: (i) written notice of any changes in the Authorized Persons' qualification as an Authorized Person within two (2) business days of such change; (ii) written confirmation to any inquiry by ISO regarding the status or identification of any specific Authorized Person within two (2) business days of such request, and (iii) periodic written updates, no less often than semi-annually, containing the names of all Authorized Persons appointed by the Authorized Commission.

3. **Protection of Confidential Market Information.**

a. The Authorized Commission has adequate internal procedures, to protect against the release of any Confidential Market Information by the Authorized Persons or other employee or agent of the Authorized Commission, and the Authorized Commission and the Authorized Persons will strictly enforce and periodically review all such procedures. In the event that ISO terminates a Non-Disclosure Agreement with an Authorized Person, and does not restore such individual's status as an Authorized Person, then the Authorized Commission shall review such internal procedures.

b. The Authorized Commission has legal authority to protect the confidentiality of Confidential Market Information from public release or disclosure and/or from release or

disclosure to any other person or entity, either by the Authorized Commission or the Authorized Persons, as agents of the Authorized Commission.

c. The Authorized Commission shall ensure that Confidential Market Information and shall be maintained by, and accessible only to, the Authorized Persons.

d. The Authorized Commission and its Authorized Person(s) shall not disclose the Confidential Market Information.

4. Defense Against Requests for Disclosure. The Authorized Commission shall defend against, and will direct the Authorized Persons to defend against, disclosure of any Confidential Market Information pursuant to any Third Party Request through all available legal process, including, but not limited to, obtaining any necessary protective orders. The Authorized Commission shall provide ISO with prompt notice of any such Third Party Request or legal proceedings, and shall consult with ISO and/or any Affected Governance Participant in its efforts to deny the request or defend against such legal process. In the event a protective order or other remedy is denied, the Authorized Commission agrees to furnish only that portion of the Confidential Market Information which their legal counsel advises ISO (and of which ISO shall, in turn, advise any Affected Member) in writing is legally required to be furnished, and to exercise then-best efforts to obtain assurance that confidential treatment will be accorded to such Confidential Market Information.

5. Use and Destruction of Confidential Market Information.

a. The Authorized Commission shall use, and allow the use of, the Confidential Market Information solely for the purpose of assisting the Authorized Commission in discharging its legal responsibility to monitor the wholesale and retail electricity markets, operations, transmission planning and siting, and generation planning and siting materially affecting retail customers within the State in which the Authorized Commission has regulatory jurisdiction, and for no other purpose. Without limiting the foregoing, the Authorized Commission shall not use its right to acquire Confidential Market Information as a means of conducting discovery or providing evidence during an adversarial proceeding against an Affected Governance Participant or any group of Participants. The Authorized Commission, however, shall not be prevented from using in an adversarial proceeding Confidential Market Information the Authorized Commission has obtained if: (i) such information becomes known in that proceeding through disclosure by entities other than the Authorized Commission; and (ii) the Authorized Commission discloses such

Confidential Market Information consistent with the protections and procedures governing the disclosure of Confidential Market Information to parties in that proceeding; or (iii) the information being disclosed no longer meets the definition of Confidential Market Information.

b. Upon completion of the inquiry or investigation referred to in any Information Request initiated by or on behalf of the Authorized Commission, or for any reason any Authorized Person is, or will no longer be an Authorized Person, the Authorized Commission will ensure that such Authorized Person either (a) returns the Confidential Market Information and all copies thereof to ISO, or (b) provides a certification that the Authorized Person and/or the Authorized Commission has destroyed all paper copies and deleted all electronic copies of the Confidential Market Information, unless such actions are inconsistent with or prohibited by applicable state law, in which case the Authorized Commission shall continue to maintain the confidentiality of the Confidential Market Information in accordance with the terms and conditions of this Certification.

6. **Notice of Disclosure of Confidential Market Information.** The Authorized Commission shall promptly notify ISO of any inadvertent or intentional release or possible release of the Confidential Market Information provided to any Authorized Person, and shall take all available steps to minimize any further release of Confidential Market Information and/or retrieve any Confidential Market Information that may have been released.

7. **Ownership and Privilege.** Nothing in this Certification, or incident to the provision of Confidential Market Information to the Authorized Person pursuant to any Information Request, is intended, nor shall it be deemed, to be a waiver or abandonment of any legal privilege that may be asserted against subsequent disclosure or discovery in any formal proceeding or investigation. Moreover, no transfer or creation of ownership rights in any intellectual property comprising Confidential Market Information is intended or shall be inferred by the disclosure of Confidential Market Information by ISO, and any and all intellectual property comprising Confidential Market Information disclosed and any derivations thereof shall continue to be the exclusive intellectual property of ISO and/or the Affected Governance Participant.

Executed, as of the date first set out above.

[Commission]

By:_____

Its:_____

[SEE NEXT PAGE]

EXHIBIT A

CERTIFICATION LIST OF AUTHORIZED PERSONS

Name of Authority	Mailing Address	Email	Tel #	Scope and Duration

APPENDIX C

FORM OF ACADEMIC INSTITUTION NON-DISCLOSURE AGREEMENT

THIS NON-DISCLOSURE AGREEMENT (the "Agreement") is made this _____ day of _____, 200_, by and between _____, (the "Authorized Institution"), with offices at _____ and ISO New England Inc., a Delaware corporation, with offices at One Sullivan Road, Holyoke, Massachusetts, 01040-2841 (the "ISO"). The Authorized Institution and the ISO shall be referred to herein individually as a "Party," or collectively as the "Parties."

RECITALS

Whereas, the ISO serves as the Regional Transmission Organization for the New England Control Area, and operates and oversees wholesale markets for electricity pursuant to the requirements of the ISO Tariff, as defined below; and

Whereas, the External Market Monitor (as defined below) serves as the independent market monitor for ISO's wholesale markets for electricity, and

Whereas, the ISO New England Information Policy requires that the ISO and the External Market Monitor maintain the confidentiality of Confidential Market Information; and

Whereas, the ISO New England Information Policy permits the ISO and the External Market Monitor to disclose Confidential Market Information to the Authorized Institution upon satisfaction of conditions stated in the ISO New England Information Policy, including, but not limited to, the execution of this Agreement by the Authorized Institution and the maintenance of the confidentiality of such information by the Authorized Institution pursuant to the terms of this Agreement; and

Whereas, the ISO desires to provide the Authorized Institution with access to Confidential Market Information, consistent with the ISO's and the External Market Monitor's obligations and duties under the ISO New England Information Policy, the ISO Tariff and other applicable FERC directives; and

Whereas, this Agreement is a statement of the conditions and requirements, consistent with the requirements of the ISO New England Information Policy, whereby the ISO may provide Confidential Market Information to the Authorized Institution.

NOW, THEREFORE, intending to be legally bound, the Parties hereby agree as follows:

1. Definitions. Capitalized terms not otherwise defined herein shall have the meanings ascribed thereto in the ISO Tariff.

1.1 Affected Governance Participant. A Governance Participant, which as a result of its participation in the markets administered by the ISO, provided Confidential Market Information to the ISO, which Confidential Market Information is requested by, or is disclosed to an Authorized Institution under this Agreement.

1.2 Authorized Researcher. Shall have the meaning set forth in the ISO New England Information Policy.

1.3 Confidential Market Information. Shall mean *Confidential Information* (as defined in the ISO New England Information Policy) consisting of market data relating to the markets administered by the ISO, including data supplied by Governance Participants and aggregate data regularly compiled by the ISO. Confidential Market Information shall not include the following categories of information without excluding any objective market data associated with them that would otherwise be provided under the first sentence of this definition: (i) draft versions of reports and analyses, (ii) internal ISO documents not related to market data, (iii) attorney-client communications, (iv) attorney work-product privileged information, (v) communications about Confidential Market Information between an Affected Governance Participant and the ISO/External Market Monitor, except to the extent that the communications become part of final written reports or final written analyses by the ISO/External Market Monitor, (vi) communications between an Affected Governance Participant and the ISO made on a confidential basis as part of a settlement proceeding or negotiation, and (vii) information provided to the ISO on a confidential basis as part of an Alternative Dispute Resolution proceeding. If the aforementioned information in (i) through (vii) is furnished to the Authorized Institution, such information shall be protected according to the terms of this Agreement, and the Authorized Institution shall return such information to the ISO as promptly as possible.

1.4 Competitive Duty Personnel. Shall mean a person whose duties include (i) the marketing or sale of electric power at wholesale; (ii) the purchase or resale of electric power at wholesale; (iii) the direct supervision of any employee with duties specified in subparagraph (i) or (ii) of this paragraph; or (iv) the provision of electricity marketing consulting services to entities engaged in the sale or purchase of electric power at wholesale.

1.5 FERC. The Federal Energy Regulatory Commission.

1.6 External Market Monitor. Shall have the meaning set forth in the ISO Tariff.

1.7 Governance Participant. Shall have the meaning set forth in the ISO Tariff.

1.8 ISO New England Information Policy. Shall have the meaning set forth in the ISO Tariff.

1.9 Information Request. A written request by the Authorized Institution in accordance with the terms of this Agreement for disclosure of Confidential Market Information pursuant to Section 3.4 of the ISO New England Information Policy.

1.10 ISO Tariff. The ISO's Transmission, Markets and Services Tariff, as it may be amended from time to time.

1.11 Non-Disclosure Certificate. Shall mean the certificate annexed hereto by which Authorized Researchers who have been granted access to Confidential Market Information shall certify their understanding that such access to Confidential Market Information is provided pursuant to the terms and restrictions of this Agreement, that they are not Competitive Duty Personnel, and that they have read this Agreement and agree to be bound by it.

1.12 Notes of Confidential Market Information. Shall mean memoranda, handwritten notes, or any other form of information (including electronic form) which copies or discloses materials described in the definition of Confidential Market Information set forth above. Notes of Confidential Market Information are subject to the same restrictions provided in this Agreement for Confidential Market Information except as specifically provided in this Agreement.

1.13 Proposed Research. Shall have the meaning set forth in Section 3.4 of the Information Policy.

1.14 Third Party Request. Any request or demand by any entity upon the Authorized Institution for release or disclosure of Confidential Market Information. A Third Party Request shall include, but shall not be limited to, any subpoena, discovery request, or other request for Confidential Market Information made by any: (i) federal, state, or local governmental subdivision, department, official, agency or court, or (ii) arbitration panel, business, company, entity or individual.

2. Protection of Confidentiality.

2.1 Duty to Not Disclose. The Authorized Institution represents and warrants that it: (i) is duly authorized to enter into and perform this Agreement; (ii) has adequate procedures to protect against the release of Confidential Market Information; and (iii) is familiar with, and will comply with, all such applicable procedures. The Authorized Institution hereby covenants and agrees not to disclose the Confidential Market Information and to deny any Third Party Request and defend against any legal process that seeks the release of Confidential Market Information in contravention of the terms of this Agreement.

2.2 Defense Against Third Party Requests. The Authorized Institution shall defend against any disclosure of Confidential Market Information pursuant to any Third Party Request through all available legal process, including, but not limited to, obtaining any necessary protective orders. The Authorized Institution shall provide the ISO, and the ISO shall provide each Affected Governance Participant and counsel for the Participants Committee, with prompt notice of any such Third Party Request or legal proceedings, and shall consult with the ISO and/or any Affected Governance Participant in its efforts to deny the request or defend against such legal process. In the event a protective order or other remedy is denied, the Authorized Institution agrees to furnish only that portion of the Confidential Market Information which its legal counsel advises the ISO (and of which the ISO shall, in turn, advise any Affected Governance Participants) in writing is legally required to be furnished, and to exercise its best efforts to obtain assurance that confidential treatment will be accorded to such Confidential Market Information.

2.3 Care and Use of Confidential Market Information.

2.3.1 Control of Confidential Market Information. The Authorized Institution shall be the custodian of any and all Confidential Market Information received pursuant to the terms of this Agreement from the ISO or the External Market Monitor.

2.3.2 Access to Confidential Market Information. The Authorized Institution shall ensure that Confidential Market Information received by that Authorized Institution is disseminated only to those persons publicly identified as Authorized Researchers in the applicable Information Request, and that such Authorized Researchers have been advised of the confidential nature of the Confidential Market Information and have agreed to abide by the terms of this Agreement by signing a Non-Disclosure Certificate. The Authorized Institution agrees that it shall be liable for any breach of this Agreement by any of the Authorized Researchers.

2.3.3 Competitive Duty Personnel. If any person who has been an "Authorized Researcher" subsequently becomes Competitive Duty Personnel, that person shall thereafter have no access to Confidential Market Information, shall return all such materials to the Authorized Institution, and shall continue to comply with the requirements set forth in this Non-Disclosure Agreement with respect to Confidential Market Information to which such person previously had access.

2.3.4 Use of Confidential Market Information. The Authorized Institution shall use the Confidential Market Information solely for the purpose of the Proposed Research. An Authorized Researcher may make copies of Confidential Market Information, but such copies become Confidential Market Information. An Authorized Researcher may make notes of Confidential Market Information, which shall be treated as Notes of Confidential Market Information if they disclose the contents of Confidential Market Information. In the event that the Authorized Institution or any Authorized Researcher desires to publish any material related to or that relies upon the Confidential Market Information, the Authorized Institution or Authorized Researcher must ensure that the Confidential Market Information is sufficiently redacted or summarized so that it may not be identified. Any such publication must be approved in writing by the ISO in advance of its release.

2.3.5 Return of Confidential Market Information. Upon completion of the Proposed Research, or upon termination of this Agreement for any reason, the Authorized Institution shall (a) return the Confidential Market Information and all copies thereof to the ISO, or (b) provide a certification that the Authorized Institution has destroyed all paper copies and deleted all electronic copies of the Confidential Market Information. The ISO may waive this condition in writing if such Confidential Market

Information has become publicly available or non-confidential in the course of business or pursuant to the ISO Tariff or order of the FERC.

2.3.6 Notice of Disclosures. The Authorized Institution shall promptly notify the ISO, and the ISO shall promptly notify any Affected Governance Participant, of any inadvertent or intentional release or possible release of the Confidential Market Information provided pursuant to this Agreement. The Authorized Institution shall take all steps to minimize any further release of Confidential Market Information, and shall take reasonable steps to attempt to retrieve any Confidential Market Information that may have been released.

2.4 Ownership and Privilege. Nothing in this Agreement, or incident to the provision of Confidential Market Information to the Authorized Institution pursuant to any Information Request, is intended, nor shall it be deemed, to be a waiver or abandonment of any legal privilege that may be asserted against, subsequent disclosure or discovery in any formal proceeding or investigation. Moreover, no transfer or creation of ownership rights in any intellectual property comprising Confidential Market Information is intended or shall be inferred by the disclosure of Confidential Market Information by the ISO, and any and all intellectual property comprising Confidential Market Information disclosed and any derivations thereof shall continue to be the exclusive intellectual property of the ISO and/or the Affected Governance Participant.

3. Remedies.

3.1 Material Breach. The Authorized Institution agrees that any release of Confidential Market Information to persons not authorized to receive it or any publication of any material related to or that relies upon the Confidential Market Information which is not (i) approved in writing by the ISO prior to publication and (ii) redacted or summarized in such a manner that the Confidential Market Information may not be identified shall constitute a breach of this Agreement and may cause irreparable harm to the ISO and/or the Affected Governance Participant. In the event of a breach of this Agreement by the Authorized Institution, the ISO may terminate this Agreement upon written notice to the Authorized Institution, and all rights of the Authorized Institution hereunder shall thereupon terminate; provided, however, that the ISO may restore status as an Authorized Institution after consulting with the Affected Governance Participant and to the extent that: (i) the ISO determines that the disclosure was not due to the intentional, reckless or negligent action or omission of the Authorized Institution; (ii) there were no harm or damages suffered by the Affected Governance Participant; or (iii) similar good cause shown.

Notwithstanding the foregoing, the Authorized Institution hereby shall indemnify, save, hold harmless, discharge, and release the ISO and each affected Governance Participant from and against any and all payments, liabilities, damages, losses or costs and expenses paid or directly incurred by the ISO and/or each affected Governance Participant arising from, based upon, related to, or associated with the breach of, or failure to perform or satisfy, any obligation of the Authorized Institution set forth in this Agreement.

3.2 Judicial Recourse. In the event of any breach of this Agreement, the ISO, the Affected Governance Participant and/or the Participants Committee shall have the right to seek and obtain at least the following types of relief: (a) temporary, preliminary, and/or permanent injunctive relief with respect to any breach and (b) the immediate return of all Confidential Market Information to the ISO. The Authorized Institution expressly agrees that in the event of a breach of this Agreement, any relief sought properly includes, but shall not be limited to, the immediate return of all Confidential Market Information to the ISO.

4. Jurisdiction. The Parties agree that jurisdiction over all other actions and requested relief with respect to the Agreement shall lie in any court of competent jurisdiction.

5. Notices. All notices required pursuant to the terms of this Agreement shall be in writing, and served at the following addresses or email addresses:

If to the Authorized Institution:

-

_____

—

_____

—

_____

—

(email address)

_____

—

_____

—

with a copy to

(email address)

If to Counsel for the Participants Committee:

(email address)

with a copy to

(email address)

If to ISO:

(email address)

with a copy to

(email address)

6. Severability and Survival. In the event any provision of this Agreement is determined to be unenforceable as a matter of law, the Parties intend that all other provisions of this Agreement remain in full force and effect in accordance with their terms.

7. Representations. The undersigned represent and warrant that they are vested with all necessary corporate, statutory and/or regulatory authority to execute and deliver this Agreement, and to perform all of the obligations and duties contained herein.

8. Third Party Beneficiaries. The Parties specifically agree and acknowledge that each Governance Participant is an intended third party beneficiary of this Agreement entitled to enforce its provisions.

9. Counterparts. This Agreement may be executed in counterparts and all such counterparts together shall be deemed to constitute a single executed original.

10. Amendment. This Agreement may not be amended except by written agreement executed by authorized representatives of the Parties.

ISO NEW ENGLAND INC.	AUTHORIZED INSTITUTION
By:	By:
_____	_____
Name:	Name:
Title:	Title:

NON-DISCLOSURE CERTIFICATE

I hereby certify my understanding that access to Confidential Market Information is provided to me pursuant to the terms and restrictions of the attached Non-Disclosure Agreement, that I have read such Non-Disclosure Agreement, and that I agree to be bound by it. In addition, I hereby certify that I am not a Competitive Duty Personnel as that term is defined in the Non-Disclosure Agreement. I understand that the contents of the Confidential Market Information, any notes or other memoranda, or any other form of information that copies or discloses Confidential Market Information shall not be disclosed to anyone other than in accordance with that Non-Disclosure Agreement.

By:

_____

Title:

_____

Representing:

_____

Date:_____

__

[NOTICE ADDRESS]