Physical & Cyber Safety Rules–Electric

Puc 201.06 Requests for Confidential Treatment of Documents Submitted by Utilities in Routine Filings.

(a) The following shall be the routine filings to which the procedure established by Puc 201.06 and Puc 201.07 applies:

(16) Utilities' cybersecurity plans;

(17) Utilities' physical security plans;

Puc 306.06 Notification of Accidents and Property Damage.

(d) A utility shall notify the commission by telephone as soon as possible, but no later than 2 hours after becoming aware of an accident or event that:

(2) Involves a breach of security or threat against the utility's facilities addressed in section 306.10;

Puc 306.10 Physical and Cyber Security Plans, Procedures and Reporting.

(a) Each utility shall develop, maintain and follow a written physical security plan designed to protect the utility's critical equipment and facilities from breaches of security. For purposes of this section, "critical equipment and facilities" means utility infrastructure without which the utility could not provide safe and reliable service to its customers.

(b) The plan shall be risk-based and incorporate:

(1) A threat level assessment;

(2) A list of critical equipment and facilities to which the plan applies;

(3) Defined security measures for critical equipment and facilities;

(4) Response procedures and notifications upon discovery of a breach in security;

(5) Defined process to track events; and

(c) Each utility shall develop, maintain and follow a written information cyber security plan designed to protect the utility's critical cyber assets. For purposes of this section, "critical cyber assets" means those electronic data, communications, and computer network systems without which the utility could not provide safe reliable service to its customers.

(d) The plan shall be risk-based and incorporate:

(1) A threat level assessment;

(2) A list of critical cyber assets;

(3) Defined security measures for critical cyber assets;

(4) Response procedures and notifications upon discovery of a breach in security;

(5) Defined process to track events; and

(6) Employee awareness training programs.

(e) Each utility shall submit to the commission annually one original and one electronic copy of each of its physical security plan and cyber security plan. If any such plan contains confidential information, the utility shall so notify the commission in writing to provide the commission with an opportunity to review the confidential information at the utility's offices in New Hampshire.

(f) On the 15th day of the month following the last day of each quarter, each utility shall file Form E-37 Quarterly Report of Equipment Theft, Sabotage and Breaches of Security, pursuant to Puc 308.17 reporting all material breaches of security as defined within the plans.

Puc 308.17 Quarterly Report of Equipment Theft, Sabotage and Breaches of Security.

Each utility shall on a quarterly basis complete a report of equipment theft, sabotage and breaches of security on Form E-37 dated 1/2015 and available at the commission website at www.puc.nh.gov, and file one signed original and one electronic copy with the commission.