RULES
OF
THE TENNESSEE PUBLIC UTILITY COMMISSION

CHAPTER 1220-04-15
UTILITY CYBERSECURITY PLANS & REPORTING

TABLE OF CONTENTS

1220-04-15-.01 DEFINITIONS.

(1) Commission – The Tennessee Public Utility Commission.

(2) Cybersecurity Incident – An event that, without lawful authority, jeopardizes, disrupts, or otherwise impacts, or is reasonably likely to jeopardize, disrupt, or otherwise impact, the integrity, confidentiality, or availability of computers, information, or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the owner/operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).

(3) Cybersecurity Plan – A plan or plans intended to protect the utility's information technology and operational technology systems from unauthorized use, alteration, ransom, or destruction of electronic data.

(4) Information Technology System – Any services, equipment, or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that falls within the responsibility of the owner/operator to operate and maintain.

(5) Operational Technology System – A general term that encompasses several types of control systems, including industrial control systems, supervisory control and data acquisition systems, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment.

(6) Sworn Statement – A written statement made under oath that the statement is true based on personal knowledge.

(7) Utility – A public utility defined by T.C.A. § 65-4-101 that provides electric, water, wastewater, or natural gas services.

Authority: *T.C.A. §§ 65-2-102, 65-4-101, and 65-4-127.* ***Administrative History:*** *New rules filed June 27, 2023; effective September 25, 2023.*

1220-04-15-.02 CONFIDENTIALITY.

All documentation submitted in accordance with T.C.A. § 65-4-127 and these rules shall be treated as confidential and shall not be open for public inspection. The Commission shall treat this documentation consistent with any federal law, regulation, or rule that protects sensitive security information or similarly designated information regarding cybersecurity.

Authority: *T.C.A. §§ 10-7-504(a)(21)(A)(i); 10-7-504(a)(21)(C)(iii); 65-2-102; and 65-4-127.* ***Administrative History:*** *New rules filed June 27, 2023; effective September 25, 2023.*

1220-04-15-.03 CYBERSECURITY PLAN.

(1) By July 1, 2023, or within one (1) year after a utility is formed, whichever is later, a utility shall prepare and implement a cybersecurity plan.

(2) Cybersecurity plans implemented in compliance with these rules must be assessed and updated by the utility no less frequently than once every two (2) years to address new threats.

Authority: *T.C.A. §§ 65-2-102 and 65-4-127.* ***Administrative History:*** *New rules filed June 27, 2023; effective September 25, 2023.*

1220-04-15-.04 ANNUAL FILING REQUIREMENTS.

(1) By July 1st of each calendar year, all utilities shall submit documentation that the utility has prepared and implemented a cybersecurity plan. At a minimum, the documentation shall include:

(a) Contact information for utility employee(s) responsible for cybersecurity;

(b) A statement indicating whether the utility conducts annual cybersecurity training for the utility personnel with access to any utility Information Technology System or Operational Technology System; and

(c) A statement indicating whether the utility has procured cybersecurity insurance.

(2) The documentation filed must include a sworn statement by the utility's chief executive officer, president, or another person with an equivalent role and authority, over the development and implementation of the cybersecurity plan. Such statement shall, at a minimum, confirm that:

(a) The utility has prepared and implemented the cybersecurity plan described in the filing;

(b) The cybersecurity plan has been prepared or updated within the last two (2) years; and

(c) All documentation and information filed is current and accurate.

Authority: *T.C.A. §§ 65-2-102 and 65-4-127.* ***Administrative History:*** *New rules filed June 27, 2023; effective September 25, 2023.*

1220-04-15-.05 FAILURE TO COMPLY; SANCTIONS.

(1) A utility fails to comply with these rules, and is considered in non-compliance, when:

(a) The company does not file documentation required by these rules showing that it has prepared a cybersecurity plan by July 1 of each calendar year; or

(Rule 1220-04-15-.05, continued)

(b) The company does not file documentation required by these rules showing that it has implemented that cybersecurity plan by July 1 of each calendar year.

(2) After a hearing, the Commission may impose reasonable sanctions, including civil and monetary penalties, against a utility in non-compliance with these rules.

(3) Monetary penalties imposed by the Commission will be consistent with the statutory limit set in T.C.A. § 65-4-120.

(4) If the Commission determines that sanctions shall include a monetary penalty, it may consider:

(a) The efforts by the utility to comply with these rules;

(b) The financial stability of the utility; and

(c) The impact of non-compliance on customers of the utility.

(5) The Commission may require a utility to establish a separate fund to further support its compliance with these rules.

(6) Any utility in non-compliance shall be reported to the General Assembly in accordance with T.C.A. § 65-4-127(f).

Authority: *T.C.A. §§ 65-2-102, 65-4-120, and 65-4-127.* ***Administrative History:*** *New rules filed June 27, 2023; effective September 25, 2023.*

1220-04-15-.06 REQUIRED NOTIFICATION TO THE COMMISSION OF CYBERSECURITY INCIDENT.

A utility shall electronically notify the Commission's Executive Director of any cybersecurity incident that results in interruption of service within 72 hours after discovery and confirmation, unless prohibited or recommended by law enforcement to avoid compromising an investigation. In such event, notification shall be required within 24 hours after such restriction is lifted by law enforcement.

Authority: *T.C.A. §§ 65-2-102 and 65-4-127.* ***Administrative History:*** *New rules filed June 27, 2023; effective September 25, 2023.*

1220-04-15-.07 COST RECOVERY FOR CYBERSECURITY INVESTMENT.

(1) To the extent that costs related to action required by this rule are not already recovered in rates, the utility may seek cost recovery:

(a) By filing a petition pursuant to T.C.A. § 65-5-103; or

(b) If permissible, by requesting an alternative regulatory mechanism pursuant to T.C.A. § 65-5-103(d).

Authority: *T.C.A. §§ 65-2-102, 65-4-127, and 65-5-103.* ***Administrative History:*** *New rules filed June 27, 2023; effective September 25, 2023.*