

TENNESSEE PUBLIC UTILITY COMMISSION



Andrew Jackson State Office Bldg.
502 Deaderick Street, 4th Floor
Nashville, TN 37243-0001

NOTICE OF PROCEDURE FOR FILING REQUIRED ANNUAL CYBERSECURITY COMPLIANCE PLAN REPORTING

Public Chapter 1111 was signed into law on June 1, 2022 and codified in T.C.A. § 65-4-127. Since that time, the Commission has engaged in the rulemaking process and, on May 8, 2023, adopted a rule for the implementation of the statute in Docket Number 23-00001. As of June 23, 2023, the rule has not been finalized and placed into effect. A copy of the proposed rule is attached for convenience.


In order to comply with T.C.A. § 65-4-127, every Commission-regulated electric, water, wastewater, and natural gas public utility must submit, annually by July 1, documentation verifying that it has implemented a cybersecurity plan. Proposed TPUC Rule 1220-4-15-.04 (see attached) describes the content of the annual compliance filing, which includes:

- (a) contact information for utility employee(s) responsible for cybersecurity;
- (b) a statement indicating whether the utility conducts annual cybersecurity training for 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.

In addition, the filing must include a notarized affidavit swearing to the accuracy and truthfulness of the contents of the filing made under oath by the utility's chief executive officer, president, or another person with an equivalent role and authority with respect to the cybersecurity plan. The affidavit must include that the utility: (a) 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) that all documentation and information filed is current and accurate.

All utility cybersecurity compliance filings should be sent to the Commission via email, with the subject line, "**Annual PC1111 Compliance Filing**," to TPUC.RulesCompliance@TN.gov. In the event that a utility is unable to submit its compliance filing electronically, please contact Jerry Kettles at (615) 770-6894. Do not include a copy of the cybersecurity plan as part of the submission.

FOR THE TENNESSEE PUBLIC UTILITY COMMISSION:



Kelly Cashman Grams, General Counsel
Dated: June 23, 2023

cc: Docket File 23-00001; TPUC Service List

**Department of State
Division of Publications**

312 Rosa L. Parks Ave., 8th Floor, Snodgrass/TN Tower
Nashville, TN 37243
Phone: 615-741-2650
Email: publications.information@tn.gov

For Department of State Use Only

Sequence Number: _____
Rule ID(s): _____
File Date: _____
Effective Date: _____

Rulemaking Hearing Rule(s) Filing Form

Rulemaking Hearing Rules are rules filed after and as a result of a rulemaking hearing (Tenn. Code Ann. § 4-5-205).

Pursuant to Tenn. Code Ann. § 4-5-229, any new fee or fee increase promulgated by state agency rule shall take effect on July 1, following the expiration of the ninety (90) day period as provided in § 4-5-207. This section shall not apply to rules that implement new fees or fee increases that are promulgated as emergency rules pursuant to § 4-5-208(a) and to subsequent rules that make permanent such emergency rules, as amended during the rulemaking process. In addition, this section shall not apply to state agencies that did not, during the preceding two (2) fiscal years, collect fees in an amount sufficient to pay the cost of operating the board, commission or entity in accordance with § 4-29-121(b).

| | |
|---------------------------------|--|
| Agency/Board/Commission: | Tennessee Public Utility Commission |
| Division: | Utilities/Legal |
| Contact Person: | Kelly Cashman-Grams, General Counsel |
| Address: | 502 Deaderick Street, 4 th Floor, Nashville, TN 37243 |
| Zip: | 37243 |
| Phone: | 615-770-6856 |
| Email: | Kelly.Grams@tn.gov |

Revision Type (check all that apply):

☐ Amendment
☒ New
☐ Repeal

☐ Content based on previous emergency rule filed on _____
☐ Content is identical to the emergency rule

Rule(s) (ALL chapters and rules contained in filing must be listed here. If needed, copy and paste additional tables to accommodate multiple chapters. Please make sure that **ALL** new rule and repealed rule numbers are listed in the chart below. Please enter only **ONE** Rule Number/Rule Title per row.)

| Chapter Number | Chapter Title |
|----------------|---|
| 1220-04-15 | Utility Cybersecurity Plans & Reporting |
| Rule Number | Rule Title |
| 1220-04-15-.01 | Definitions |
| 1220-04-15-.02 | Confidentiality |
| 1220-04-15-.03 | Cybersecurity Plan |
| 1220-04-15-.04 | Annual Filing Requirements |
| 1220-04-15-.05 | Failure to Comply; Sanctions |
| 1220-04-15-.06 | Required Notification to the Commission of Cybersecurity Incident |
| 1220-04-15-.07 | Cost Recovery for Cybersecurity Investment |

Place substance of rules and other info here. Please be sure to include a detailed explanation of the changes being made to the listed rule(s). Statutory authority must be given for each rule change. For information on formatting rules go to

<https://sos.tn.gov/products/division-publications/rulemaking-guidelines>.

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.

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. §§ 65-2-102, 65-4-127, 10-7-504(a)(21)(A)(i), and 10-7-504(a)(21)(C)(iii).

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.

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.

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
- (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 noncompliance 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.

1220-04-15-.06 REQUIRED NOTIFICATION TO COMMISSION

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.*

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.*

West's Tennessee Code Annotated

Title 65. Public Utilities and Carriers (Refs & Annos)

Chapter 4. Regulation of Public Utilities by Commission (Refs & Annos)

Part 1. General Provisions

T. C. A. § 65-4-127

§ 65-4-127. Utility cyber security plans

Effective: June 1, 2022

[Currentness](#)

(a) As used in this section:

(1) “Commission” means the Tennessee public utilities commission; and

(2) “Utility” means a public utility that provides electric, water, wastewater, or natural gas services.

(b)(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 cyber security plan to provide for the protection of the utility's facilities from unauthorized use, alteration, ransom, or destruction of electronic data. The utility shall annually submit documentation of the utility's compliance with this section to the commission by July 1.

(2) The documentation required by this section must be made in writing and under oath by the chief executive officer, president, or other person with an equivalent role of the utility.

(c) A utility shall assess and update the cyber security plan implemented pursuant to this section no less frequently than once every two (2) years to address new threats.

(d) A utility that fails to comply with this section is subject to reasonable sanctions ordered by the commission as described in rule. The fees collected from civil penalties under this section must be remitted to the commission for enforcement of this section.

(e) The commission shall enforce this section and may promulgate rules necessary to effectuate this section. The rules must be promulgated in accordance with the Uniform Administrative Procedures Act, compiled in title 4, chapter 5.

(f) The commission shall include with the annual report required under [§ 65-1-111](#), a separate report regarding compliance with this section to the chair of the commerce committee of the house of representatives, the chair of the commerce and labor committee of the senate, the department of safety, and the legislative librarian. The report must include, at a minimum, information on the utilities that have failed to comply with this section.

Credits

2022 Pub.Acts, c. 1111, § 2, eff. June 1, 2022.

T. C. A. § 65-4-127, TN ST § 65-4-127

Current with laws from the 2023 Regular Sess. of the 113th Tennessee General Assembly. Pursuant to §§ 1-1-110, 1-1-111, and 1-2-114, the Tennessee Code Commission certifies the final, official version of the Tennessee Code and, until then, may make editorial changes to the statutes. References to the updates made by the most recent legislative session should be to the Public Chapter and not to the T.C.A. until final revisions have been made to the text, numbering, and hierarchical headings on Westlaw to conform to the official text. Unless legislatively provided, section name lines are prepared by the publisher.

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.