**BEFORE THE PUBLIC SERVICE COMMISSION**
**OF THE STATE OF MISSOURI**

| | | |
|---|---|---|
| In the Matter of the Application of Evergy Metro, Inc. d/b/a Evergy Missouri Metro for Authority to Issue Debt Securities | ) ) ) | **Case No. EF-2026-0206** |

**STAFF'S RESPONSE TO EVERGY MISSOURI METRO'S MOTION FOR PROTECTIVE ORDER AND FOR EXPEDITED TREATMENT**

**COMES NOW** the Staff of the Missouri Public Service Commission ("Staff"), by and through counsel, and responds to Evergy Metro, Inc. d/b/a Evergy Missouri Metro's ("Evergy") Motion for Protective Order and for Expedited Treatment ("Motion"). Staff does not oppose reasonable safeguards against the unauthorized disclosure of information that actually qualifies as confidential or highly confidential. The Motion should nevertheless be denied. It seeks to control the analytical methods of other parties, including the Commission's own legal and technical staff. It also fails to identify particular information requiring greater protection, fails to show that the Commission's existing confidentiality rule is inadequate, shifts Evergy's own designation obligations to recipients, operates asymmetrically, and does not justify expedited final relief.

## I. THE EXISTING RULE ALLOCATES THE RESPONSIBILITIES CORRECTLY

1. The Motion broadly asserts that Confidential and Highly Confidential protections under 20 CSR 4240-2.135 are inadequate for artificial intelligence "(AI") risks. However, Staff asserts the Commission's existing confidentiality rule already states the controlling obligation: every person with access to protected information must keep it secure and may neither use nor disclose it except for preparation and conduct of the proceeding. 20 CSR 4240-2.135(13). The issue is therefore not whether confidential information must be

protected. It must be. The issue is whether Evergy has shown a need to superimpose a separate, technology-specific regime upon every item it labels “Confidential” or “Highly Confidential.”

2. The rule first places the designation burden upon the producing party. Rule 20 CSR 4240-2.135(2)(A) identifies the categories that may be designated confidential without a separate protective order. Section (2)(B) requires the claimant to identify the category, explain why it applies, and designate only the particular information that qualifies. Section (18) represents to the Commission that the claim rests upon a reasonable and good-faith belief that the information is confidential under the cited provision.

3. Information does not become confidential merely because disclosure may embarrass Evergy, place the company or its dealings in an unfavorable light, or create controversy. It must actually fall within a protected category — for example, customer-specific information, qualifying personnel or market information, negotiating strategies, facility-security information, protected professional work, or trade secrets. Evergy controls its records and is best situated to identify, segregate, and explain the portions that qualify.

4. The proper allocation is therefore straightforward. Evergy must disclose the evidence the Commission requires, must designate only the portions that legitimately qualify for confidential treatment, and must invoke the existing rule to protect that information from outside disclosure. Staff, and all other parties, must maintain that protection while examining the evidence and advising the Commission. The solution is not

to curtail AI or another class of analytical tools, but to enforce the confidentiality duties that already govern both the producer and the recipient.

5. The rule protects information against risk; it does not regulate technology by name.[1] A tool that transmits protected information to an unauthorized person, retains it for an unauthorized purpose, or uses it outside this proceeding may violate section (13) of the Commission's Confidentiality rule, whether the tool is described as AI, email, cloud storage, document management, remote access, transcription, or something else. Conversely, a secure analytical tool does not become unlawful merely because it is generative or hosted by a service provider operating under enforceable access, non-training, non-retention, and deletion restrictions.

6. Evergy identifies no actual unauthorized disclosure, threatened disclosure, particular tool presently being used, or specific category of information for which the existing rule has proved inadequate. It does not analyze the protection already supplied by section (13) of the Commission's Confidentiality rule and does not attempt to show why that protection cannot address the asserted risk. Instead, the Motion would make Evergy's label a substitute for both a valid confidentiality designation and a showing that greater protection is necessary.

[1] This technology-neutral approach is preferable as it provides consistent protection while allowing the Commission to employ the most effective analytical tools available. Evergy's request for AI-specific restrictions could be seen as creating a precedent requiring separate protective orders for each new analytical technology, potentially impairing the Commission's ability to keep pace with technological developments in regulatory analysis.

## II. EVERGY HAS NOT MADE THE REQUIRED PARTICULARIZED SHOWING

7. Rule 20 CSR 4240-2.135(4) permits protection greater than an ordinary confidential designation only upon a motion explaining: (1) what information must be protected; (2) the harm to the disclosing entity or the public that might result from disclosure; and (3) how the information may be disclosed while protecting the interests of the disclosing entity and the public. That is a particularized inquiry directed to identified information and identified harm.

8. The Motion makes no such showing. It refers generically to information that may be produced in discovery and asks that every present and future designation automatically carry an additional restriction upon AI processing. It does not identify the information, the recognized harm that disclosure would cause, the inadequacy of ordinary safeguards, or the least restrictive means of addressing the asserted risk.

9. The proposed order would thus convert the exception in section (4) into the default. The unilateral act of designation would immediately control the Commission's internal analytical methods before Evergy had established either that the information qualifies as confidential or that ordinary protection is insufficient. Section (4) does not permit that result.

10. The Commission should deny the Motion without prejudice. Should Evergy later identify particular information and demonstrate a concrete need for greater protection, the Commission can consider a narrowly tailored request under the procedure the rule already provides.

## III. THE PROPOSED ORDER IS ASYMMETRIC AND INTRUSIVE

11. The Motion is facially reciprocal because it speaks of "any party," but its practical operation is one-sided. Under its proposal, Evergy may use AI to collect, organize, summarize, and analyze its own confidential operational records because it is not a receiving party to whom those records were disclosed. Staff and the other participants charged with testing the same evidence would potentially be restricted from using functionally comparable tools. A situation where Evergy would retain modern analytical capacity while limiting the Commission's capacity to examine Evergy's claims could occur.

12. The proposed "exclusive control" exception compounds the inequality. It favors an enterprise able to purchase and maintain private infrastructure and may exclude secure commercial services solely because a service provider owns or operates the servers. Server ownership is not a substitute for a functional security analysis. "Third-party hosted" does not mean "public," and "generative" does not mean "unsecured."

13. The certification requirement is equally misplaced. It would compel Staff and other parties to describe its tools, workflow, and security architecture to the regulated company whose evidence they are examining. Those disclosures may reveal analytical methods, resource allocation, proprietary software and vendor relationships, litigation preparation methods, or potentially work-product information. If technical documentation is ever material to a specific dispute, it should be retained by the user and submitted only to the Commission, confidentially or in camera, upon a motion and showing of good cause.

14. These conditions impose operational burdens, invite satellite disputes, and risk chilling use of efficient, compliant tools that already meet no-retention and no-training standards.

15. A protective order should prevent unauthorized disclosure. It should not allow the producing utility to approve or disapprove the analytical methods of the Commission, its counsel, engineers, or other personnel, nor of any other party. Nor should access to secure analytical technology depend upon the size of a participant's technology budget.

## IV. THE AUTHORITIES AND EXISTING PROCEDURE DO NOT SUPPORT RELIEF

16. Evergy's authorities may inform the distinction between unsecured public tools and services operating under enforceable safeguards, but they do not support the remedy requested here.[2] They concern courts regulating private litigants, lawyers, or individual users—not a regulated utility seeking authority to prescribe the tools used by the regulatory commission's own institutional staff, other government agencies, and intervening parties. None converts a general concern about unauthorized disclosure into a right to supervise the Commission's internal analysis. Looking specifically to the *Morgan* case cited by Evergy, that court required a party to retain written documentation of

[2] Evergy relies principally on Morgan v. V2X, Inc., No. 25-cv-01991-SKC-MDB, 2026 WL 864223, at *5, *7-8 (D. Colo. Mar. 30, 2026). Morgan rejected both parties' proposed language and adopted reciprocal, contract-based safeguards; it did not require servers within a litigant's exclusive control or routine certification to a designating adversary, and it cautioned against overdesignation. United States v. Heppner, 820 F. Supp. 3d 292 (S.D.N.Y. 2026), concerned a criminal defendant's use of a public AI tool. The Court of International Trade order required identification of AI-assisted text and certification against unauthorized disclosure; it did not impose the blanket prohibition sought here. Order on Artificial Intelligence, U.S. Ct. Int'l Trade (June 8, 2023). None addressed a regulated utility's attempt to prescribe the analytical tools used by the regulatory commission's own institutional staff. These authorities do not establish a Missouri Commission-specific need, do not reflect Commission practice under 20 CSR 4240-4240-2.135, and do not address how existing Commission confidentiality regimes function in this docket.

contractual protections; it did not require proactive delivery of a detailed security certification to the opposing party in every instance.[3]

17. Portions of the proposed order also conflict with the Commission's existing procedure. Evergy asks that a tool delete "all uploaded confidential information at the conclusion of the docket." Section (15) of the Commission's Confidentiality rule, however, addresses return or destruction after completion of the proceeding, including judicial review, and section (16) separately governs Commission and Office of the Public Counsel officers and employees under section 386.480, RSMo. Any order must also preserve applicable public-record duties, litigation holds, and ordinary system backups that cannot reasonably be altered without compromising system integrity.

18. The Motion further invokes sections 476.110 and 476.120, RSMo, which describe contempt powers and punishment available to a "court of record." An agency's recourse for contemptuous conduct in a contested case is addressed by section 536.095, RSMo, through application to the circuit court. A protective order should state the duties imposed and the remedies lawfully available; it should not imply an enlargement of the Commission's statutory authority.

## V. EXPEDITED FINAL RELIEF IS NOT JUSTIFIED

19. Rule 20 CSR 4240-2.080(14) requires a motion for expedited treatment to state with particularity the requested action date, the harm avoided or benefit obtained, the negative effect—or absence of negative effect—on customers or the public, and that the

[3] *Morgan* at p. 14.

pleading was filed as soon as it could have been. Evergy provides a date and a generalized assertion of risk, but identifies no imminent disclosure, does not address the effect on customers or the public, and does not explain why a concern reflected in authorities dating to 2023 could not have been raised earlier.

20. The requested order would immediately affect the Commission's and the parties' analytical methods, costs, discovery review, and ability to respond to confidential evidence. It would attach those consequences to Evergy's unilateral designations before deciding whether the information qualifies or requires greater protection. Those consequences counsel against final relief upon an abbreviated record. There is no demonstrated emergency requiring adoption of Evergy's language on an expedited basis.

**VI. ALTERNATIVE PROCEDURE**

21. What Evergy is seeking is the same blanket order in every open Evergy West and Evergy Metro case based on a concern applicable to virtually every Commission proceeding and every utility. If Evergy's approach is accepted, other utilities could request company-specific orders in individual cases that could produce different AI standards among utilities and case files. This would create unnecessary administrative complexity, potentially impair consistent agency operations, and potentially allow individual companies to shape the technology policies of Staff, the Office of the Public Counsel, and intervening parties. If the Commission determines that an AI-specific clarification is warranted, Staff recommends that additional guidance would be better handled through:

a. A Commission-wide clarification of 20 CSR 4240-2.135;

b. A generally applicable standing order;

c. An amendment to the Commission's confidentiality rule, after stakeholder input and engagement; or

d. Standardized language for future orders.

22. That being said, in no event should a participant be required to disclose its tools, workflow, or security architecture to an adversary. Should the Commission determine that some sort of review or certification of a party's use of AI-enabled services is required, Staff recommends the Commission order any relevant documentation be retained and provided to the Commission for confidential or in camera review only upon a specific showing of good cause.

## VII. CONCLUSION

23. Staff recognizes that Evergy's concern regarding the use of public or inadequately secured AI platforms is legitimate; however, Staff recommends that the requested protective order is unnecessary as 20 CSR 4240-2.135 already requires all recipients to keep confidential, or highly confidential, secure and prohibits its unauthorized use or disclosure. Further, Staff and the Office of the Public Counsel are subject to section 386.480, RSMo.

24. Staff recommends that the proposed order be denied in its present form, as its definitions, exclusive-control requirement, certification obligation, deletion provisions, and enforcement language are overbroad or inconsistent with the Commission's existing framework. Should the Commission determine that express clarification is useful, Staff is supportive of narrowly tailored guidance confirming that confidential or highly

confidential information may not be submitted to any AI service that permits unauthorized access, model training, secondary use, or disclosure.

**WHEREFORE,** Staff respectfully requests that the Commission deny Evergy's Motion for Protective Order and deny expedited final relief; or, alternatively, issue narrowly tailored guidance confirming that confidential information may not be submitted to any AI service that permits unauthorized access, model training, secondary use, or disclosure applicable to all parties practicing before the Commission; and grant such other relief as the Commission deems just and reasonable.

Respectfully submitted,

*/s/ Mark Johnson*
**MARK JOHNSON**
Missouri Bar No. 64940
Chief Staff Counsel
**Paul T. Graham**
Senior Staff Counsel
Missouri Bar No. 30416
Missouri Public Service Commission
P.O. Box 360
Jefferson City, MO 65102
573-751-7431 (Voice)
573-751-9285 (Fax)
mark.johnson@psc.mo.gov
paul.Graham@psc.mo.gov

Attorneys for the Staff of the
Missouri Public Service Commission

## CERTIFICATE OF SERVICE

I hereby certify that copies of the foregoing have been transmitted by electronic mail to counsel of record on this 31st day of July 2026.

**/s/ *Mark Johnson***