

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

In the Matter of Evergy Metro, Inc. d/b/a	)	
Evergy Missouri Metro's Request for	)	File No. ER-2026-0143
Authority to Implement a General Rate	)	
Increase for Electric Service.	)	

RESPONSE TO EVERGY'S MOTION FOR AMENDED PROTECTIVE ORDER

Pursuant to paragraph 1 of the Missouri Public Service Commission's ("Commission") July 27, 2026 *Order Directing Response and Issuing a Preliminary Protective Order* ("Order"), Google LLC ("Google") hereby files this Response to Evergy Metro, Inc. d/b/a Evergy Missouri Metro's ("Evergy") July 17, 2026 *Motion for Protective Order and for Expedited Treatment* ("Motion for AI Protective Order"):

I. Introduction

1. Google appreciates Evergy's effort to ensure that confidential and highly confidential information exchanged in this proceeding is protected, and Google agrees that the use of unsecured or publicly accessible generative artificial intelligence ("AI") platforms to process such information poses real risks. Google's own highly confidential information has been produced in this proceeding, and Google takes the protection of that information seriously.

2. At the same time, the Commission should not adopt the restrictions Evergy proposes wholesale. Several of Evergy's proposed restrictions exceed what is necessary, are operationally unworkable, or impose ongoing compliance burdens.

3. To the extent additional clarity is warranted, such clarification should preserve the ability of parties to use secure, closed systems that are designed to protect against the very risks Evergy has identified.

II. Background

4. On February 6, 2026, Evergy filed its request for authority to implement a general

rate increase for electric service. In connection with that proceeding, parties — including Google — have submitted and exchanged substantial volumes of confidential and highly confidential information pursuant to the Commission’s rules and the April 13, 2026 Protective Order.

5. On July 17, 2026, Evergy filed its Motion for AI Protective Order citing concerns about the use of “unsecured or generative” AI tools to process confidential information and requesting amendment of the existing Protective Order in this proceeding as well as several other MPSC proceedings¹ and Kansas Corporation Commission proceedings.²

6. On July 27, 2026, the Commission preliminarily granted Evergy’s request directing that no party shall upload confidential information into unsecured or generative AI tools and directing parties to file responses no later than August 6, 2026.³

III. The Existing Confidentiality Protections in the Regulatory Framework, Protective Order, and Nondisclosure Agreement

7. Before turning to the specific deficiencies in Evergy’s proposed restrictions, it bears recognizing that robust confidentiality protections are already in place for this proceeding.

8. Commission Rule 20 CSR 4240-2.135 establishes a comprehensive framework for the handling of confidential information in Commission proceedings. Under that rule, all persons who access confidential information must first certify in writing their compliance with the rule’s requirements. *See* 20 CSR 4240-2.135(7). Access to confidential information is restricted to attorneys of record, employees acting as subject-matter experts, and designated outside experts. *See* 20 CSR 4240-2.135(6). Crucially, the rule provides that “[a]ll persons who have access to information under this rule shall keep the information secure and may neither use nor disclose such

¹ *See, e.g.*, File Nos. EA-2026-0154, EO-2026-0188, among others.

² *See, e.g.*, Docket Nos. 23-EKCE-588-TAR, 23-EKCE-775-RTS, 25-EKCE-207-PRE, 25-EKME-315-TAR, and 25-EKCE-294-RTS. Among potentially others.

³ Order Directing Responses and Issuing a Preliminary Protective Order, ¶¶ 1, 2.

information for any purpose other than preparation for and conduct of the proceeding for which the information was provided.” 20 CSR 4240-2.135(13). Additionally, within ninety (90) days after the completion of a proceeding, all copies of confidential information in the possession of any party must be returned to the designating party or destroyed. *See* 20 CSR 4240-2.135(15).

9. Layered on top of these regulatory protections, the April 13, 2026 Protective Order governing this proceeding imposes additional safeguards specifically tailored to the sensitivity of the information at issue here. The Protective Order requires every person seeking access to Confidential Information and Highly Confidential information to execute a Nondisclosure Agreement (“NDA”) certifying compliance with 20 CSR 4240-2.135 and the terms of the Protective Order. *See* Protective Order, Ordering Paragraph 2; Ex. A; Ex. B.

10. Additional protections exist for highly confidential information. The Protective Order expressly provides that “[p]ersons afforded access to materials or information designated ‘Highly Confidential’ shall neither use nor disclose such materials or information for purposes of business or competition or any other purpose other than in regard to the case referenced above and shall keep the materials and information secure and confidential.” *See* Protective Order, Ordering Paragraph 1(e)(ii). It further requires that all Highly Confidential information and notes pertaining to such information “shall be returned to the designating party or destroyed upon conclusion of the referenced case.” *See id.* ¶ 1(e)(iii).

11. Taken together, these existing protections ensure that: (i) parties are prohibited from disclosing confidential information to third parties; (ii) all parties receiving confidential information must execute NDAs; and (iii) confidential information must be returned or destroyed at the close of the proceeding. Any amended protective order addressing AI should be understood against this backdrop of already-existing obligations. The question is not whether to protect

confidential information — that obligation is firmly established — but whether Evergy’s specific proposed restrictions are needed and, if so, are they appropriately calibrated to meet the actual risks posed by AI tools.

IV. The Legal Authorities Evergy Cites Do Not Support the Restrictions Proposed

12. Evergy’s Motion relies on three sources of authority: (1) an Order on Artificial Intelligence issued by Judge Vaden of the United States Court of International Trade (“USCIT”) in 2023; (2) *Morgan v. V2X, Inc.*, 2026 WL 864223 (D. Colo. Mar. 30, 2026); and (3) *United States v. Heppner*, 820 F. Supp. 3d 292 (S.D.N.Y. Feb. 17, 2026). Each authority arose from circumstances quite different from a Commission rate proceeding. None of these cases stands for the proposition that a party should be restricted from using a fully secure, closed AI tool under stringent data processing agreements.

13. The USCIT’s 2023 Order on Artificial Intelligence addresses a specialized federal court’s concern about the use of generative AI to draft briefs and other submissions containing proprietary information in international trade litigation. The order does not purport to restrict the use of secure, closed AI systems.

14. *Morgan v. V2X, Inc.* arose over concern of a pro se plaintiff’s upload of confidential information to an unidentified AI platform in an employment discrimination case, prompting the defendant to seek disclosure of the tool and amendment of the protective order. *See Morgan*, 2026 WL 864223, at *1–2. Notably, the court did not adopt the broad restrictions the defendant sought; it declined to prohibit AI use altogether and instead fashioned an order permitting use of platforms meeting certain contractual safeguards. *Morgan*, 2026 WL 864223, at *7–8.

15. *United States v. Heppner* addressed whether a criminal defendant’s communications with the publicly available Claude platform were protected by attorney-client privilege or the work product doctrine. *Heppner*, 820 F.Supp.3d at 294–95. The court’s ruling

turned entirely on an open, public version of Claude. *See Heppner*, 820 F.Supp.3d at 296–97. The court’s analysis does not speak to a secure, closed AI system.

16. Google raises these observations not to suggest that the Commission should be indifferent to the evolving landscape of AI and confidential information. Rather, the point is that the authorities Evergy cites do not address secure, closed AI Tools, and the Commission should be cautious about importing restrictions from inapposite contexts that may carry unintended operational consequences.

V. Evergy’s Proposed Restrictions are Unworkable and Impose Burdensome Ongoing Compliance

A. The “Exclusive Control” Restriction Would Effectively Prohibit All Legitimate Secure, Closed AI Tools

17. Evergy proposes that any permissible AI tool must “not transmit, store, or retain any confidential information on servers or systems that are outside the receiving party’s exclusive control.” *See* Motion ¶ 11(a). Google understands the intuition behind this restriction, but this cannot be reconciled with how modern secure, closed AI Tools actually function.

18. The vast majority of secure, closed AI platforms — frequently referred to as enterprise-grade systems — are designed for professional use, expressly prohibit the use of customer data for model training, and operate on cloud infrastructure that is not under the “exclusive control” of the receiving party. These enterprise-grade systems are governed by stringent data processing agreements under which data is encrypted in transit and at rest, never used for training, and accessible only to authorized users.

19. These secure, closed AI systems provide parties with powerful and legitimate tools to review, analyze, and organize large volumes of information — capabilities that serve the interests of all parties, including the efficient conduct of Commission proceedings. Restrictions

that effectively preclude their use would hinder the ability of parties to perform competent and efficient work on this proceeding and would do so without commensurate benefit to the protection of confidential information.

20. Under Everyg's proposed language, a party deploying a fully secure, closed AI tool under such an agreement would technically violate the restriction because the underlying servers may be hosted by a third-party cloud provider. The practical effect would be to prohibit not merely open AI platforms that present genuine risk, but also the secure, closed systems specifically designed to prevent the unauthorized disclosure Everyg seeks to address. That outcome may not be what Everyg intends, but the language as written would produce it.

B. The Ongoing Written Certification Requirement Is Unduly Burdensome and Procedurally Undefined

21. Everyg proposes that a receiving party must provide "written certification to the designating party describing the AI Tools that the receiving party is using and the safeguards that are in place." See Motion ¶ 11(d). While a one-time certification at the outset of AI use may be reasonable, Everyg's proposal raises significant practical questions that the Motion does not answer: How is the certification submitted — directly to the designating party, to the Commission, or both? What is the applicable timeline? What is required when a party changes platforms or begins using a new AI tool during the course of the proceeding? How will the certification be implemented in this proceeding? Will all parties have to execute updated NDAs?

22. As drafted, Everyg's proposal creates the implication of a continuous certification obligation — one that would require parties to provide new written certifications every time their AI toolkit changes or evolves, which in a rapidly moving technology environment may occur frequently. That ongoing obligation is not tethered to any Commission rule or established

procedure and would impose a substantial administrative burden without corresponding benefit, particularly given the existing written certification requirements already imposed by 20 CSR 4240-2.135(7) for access to confidential information generally.

VI. If the Commission Takes Any Action, the Commission Should Permit Reasonable Use of Secure, Closed AI Tools

23. To the extent the Commission wishes to provide additional specificity in future proceedings, Google respectfully suggests that the Commission should conduct a rulemaking to modify 20 CSR 4240-2.135. Alternatively, or as a temporary measure, the simplest and most direct path to the protection Everygy seeks is an amendment to the NDA forms (Exhibits A and B) to add the following certification:

I understand and agree that the prohibition on use and disclosure of confidential information under 20 CSR 4240-2.135 and the Protective Order extends to the input, upload, or submission of confidential information to any publicly available or open generative artificial intelligence platform, including standard versions of ChatGPT, Claude, Gemini, or similar tools that are not deployed under a binding data protection agreement that (a) prohibits the provider from using customer inputs to train or improve its model, (b) prohibits disclosure of customer inputs to unauthorized third parties, and (c) allows the user to delete uploaded confidential information. Use of a secure, closed AI system operating under such an agreement is not prohibited by this certification.

24. If the Commission determines that additional specificity is warranted, the language proposed above strikes the appropriate balance and can be incorporated into NDA forms going forward and/or added to 20 CSR 4240-2.135. Google's proposed language avoids ongoing certification to the designating party and does not restrict secure, closed AI Tools with appropriate data processing agreements that allow the user to control and delete uploaded confidential information.

VII. Conclusion

WHEREFORE, Google respectfully requests the Commission decline to adopt Everygy's proposed restrictions in their current form, and, to the extent the Commission amends its Protective

Order, that it permit the use of secure, closed AI systems, and that the Commission take such other actions as the Commission deems necessary to protect confidential information while enabling the legitimate and beneficial use of modern AI tools in this proceeding.

Respectfully submitted,

POLSINELLI PC

By: /s/ Andrew O. Schulte
Andrew O. Schulte (#62194)
Frank A. Caro, Jr. (#42094)
Jared R. Jevons (#75114)
900 W. 48th Place, Suite 900
Kansas City, Missouri 64112
(816) 572-4754
aschulte@polsinelli.com
fcaro@polsinelli.com
jjevons@polsinelli.com

Attorneys for Google LLC

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing was served upon all of the parties of record or their counsel, pursuant to the Service List maintained by the Data Center of the Missouri Public Service Commission on August 6, 2026.

/s/ Andrew O. Schulte