STAFF REPORT

City of Dripping Springs

PO Box 384

511 Mercer Street

Dripping Springs, TX 78620

Submitted By: Aniz Alani, City Attorney

Council Meeting Date: December 16, 2025

Agenda Item Wording: Approval of a Resolution of the City of Dripping Springs Amending the Artificial Intelligence (AI) Policy to Restrict Use of Certain Agentic AI Tools Susceptible To Cybersecurity Vulnerabilities.

Agenda Item Requestor: IT Director

Summary/Background: On December 2, 2025, the City Council adopted a comprehensive AI Policy to guide the responsible and secure use of AI technologies by City officials, employees, contractors, and vendors. The policy establishes clear rules for permitted and prohibited uses of AI, including a process for approving new tools and a list of banned platforms.

Following adoption, the IT Director identified emerging security concerns related to AI assistants that can access, summarize, or interact with City email accounts, as well as AI-powered browsers and browser features that leverage AI to automate or summarize web sessions. These tools present unique risks, including prompt injection attacks, hidden phishing, and unauthorized access to sensitive information, which are not fully addressed by the current policy language.

The IT Director recommends amending the AI Policy to explicitly prohibit:

(a) The use of AI assistants or features that automatically summarize, read, or interact with City email accounts or email content, including but not limited to Gemini, Copilot, or similar tools, unless specifically approved by the IT Director.
(b) The use of AI-powered browsers or browser features (such as Atlas from ChatGPT, or AI browsing modes in Edge, Chrome, etc.), unless specifically approved by the IT Director. This includes any browser or extension that leverages AI to interact with, summarize, or automate tasks within web sessions.

These amendments are intended to address current and anticipated security threats, and to provide clear, enforceable guidance to staff regarding prohibited uses. The changes will be incorporated into Section 6 (Prohibited Uses), Section 11 (Exceptions), and Appendix B (Prohibited AI Platforms) of the AI Policy.The amendment will not affect the process for requesting

exceptions, which will continue to require written approval from the IT Director or City Administrator.

The amended policy and draft resolution also clarifies that the IT Director may add or remove specific tools from Appendix B via administrative update.

Commission Recommendations:	N/A
Recommended Council Actions:	Adoption of a resolution amending the City's Artificial Intelligence (AI) Policy to restrict use of certain agentic AI tools susceptible to Cybersecurity vulnerabilities as described in the meeting materials.
Attachments:	Resolution 2025-R50, including Exhibit A: Amendments to the City Artificial Intelligence (AI) Policy