



# ARTIFICIAL INTELLIGENCE (AI) POLICY

## TABLE OF CONTENTS

---

<b>POLICY SUMMARY .....</b>	<b>1</b>
1. WHAT IS THE AI POLICY & WHY IT MATTERS .....	1
1.1. <i>What is AI?</i> .....	1
1.2. <i>Main Goals of the Policy</i> .....	1
1.3. <i>Who Follows the Policy?</i> .....	1
2. RULES FOR USING AI .....	1
2.1. <i>Good AI vs. Risky AI</i> .....	1
2.2. <i>Who's in Charge?</i> .....	2
2.3. <i>What AI is Allowed?</i> .....	2
3. WHAT'S NOT ALLOWED & FINAL RULES .....	2
3.1. <i>Banned AI Uses</i> .....	2
<b>ARTIFICIAL INTELLIGENCE (AI) POLICY .....</b>	<b>4</b>
1. PURPOSE .....	4
2. TERMS & DEFINITIONS .....	4
3. SCOPE .....	6
4. GUIDING PRINCIPLES FOR RESPONSIBLE AI SYSTEMS .....	7
5. AI GOVERNANCE FRAMEWORK: MANAGEMENT, OVERSIGHT, AND ACCOUNTABILITY .....	7
6. PROHIBITED USES .....	8
7. PUBLIC-FACING AI .....	9
8. PUBLIC RECORDS .....	10
9. TRAINING .....	10
10. VIOLATIONS OF THE AI POLICY .....	10
11. EXCEPTIONS .....	10
12. PREEMPTION AND CONSTRUCTION .....	11
APPENDIX A: PERMITTED AI PLATFORMS .....	12
APPENDIX B: PROHIBITED AI PLATFORMS .....	13
APPENDIX C: AI APPROVAL REQUEST FORM .....	14



# Policy Summary

*The City of Dripping Springs' Artificial Intelligence (AI) Policy follows a model created by the GovAI Coalition, a group of cities working together to solve challenges related to using AI in government. The policy also incorporates rules from Texas state law, including those recently enacted by the 89th Texas Legislature (2025) pursuant to [H.B. 149](#), [S.B. 1964](#), [H.B. 3512](#), and [H.B. 2818](#).*

## 1. What is the AI Policy & Why It Matters

### 1.1. What is AI?

- AI (Artificial Intelligence) is when a machine or computer can make decisions, give advice, or help with tasks like writing, predicting, or sorting information.

### 1.2. Main Goals of the Policy

- (a) Help employees understand how to safely use AI
- (b) Set rules for how AI tools are chosen, used, or avoided
- (c) Ensure employees remain in control of important decisions
- (d) Stop dangerous or unfair AI use
- (e) Protect people's private information

### 1.3. Who Follows the Policy?

- (a) City employees (full-time, part-time, volunteers, interns)
- (b) Anyone who uses, manages, or buys AI tools for the City

## 2. Rules for Using AI

### 2.1. Good AI vs. Risky AI

- (a) Regular AI helps with non-critical tasks.

- (b) Heightened-Scrutiny AI makes significant decisions (like approving housing or benefits), these need extra care, review, and approval.

## 2.2. Who's in Charge?

- (a) City Council and City Administrator: Top oversight
- (b) IT Director: Manages AI tools, checks safety, gives approvals, provides training
- (c) City Attorney: Checks laws and helps with contracts
- (d) Communications Director: Makes sure the public and staff know how to report AI problems
- (e) All Employees & Officials: Must take AI training every year

## 2.3. What AI is Allowed?

- (a) *Allowed AI Tools (Appendix A), These are okay if used prudently:*
  - (i) ChatGPT: Writing, brainstorming, coding help
  - (ii) CoPilot: Helps with emails, tasks, meetings
  - (iii) Grok: Social media, trends, coding
  - (iv) Gemini – Google apps, document help, research
  - (v) Claude.ai: Writing, research, large tasks

## 3. What's Not Allowed & Final Rules

### 3.1. Banned AI Uses

- (b) *The City will NOT allow:*
  - (i) AI tools that have not been approved
  - (ii) AI that ranks people (like a “social score”) and impacts their access to services
  - (iii) AI that makes significant decisions without human intervention
  - (iv) AI that deceives people or causes harm
  - (v) AI that uses personal private information or confidential City information outside of the City’s secured computer systems (e.g., cloud-based AI).
  - (vi) AI assistants or features that automatically summarize, read, or interact with City email accounts or email content

~~(v)~~ (vii) AI-powered browsers or browser features (such as Atlas from ChatGPT, or AI browsing modes in Edge, Chrome, etc.). This includes any browser or extension that uses AI to interact with, summarize, or automate tasks within web sessions.

**(c) *AI for the Public***

- If AI is used on City websites or in services to significantly influence a consequential decision, the public must be notified on the City's website.

**(d) *Public Records***

- All records, including ones created using AI, must be maintained properly.

**(e) *Violations***

- (i) Violations of these rules may result in disciplinary action, up to and including termination of employment.
- (ii) Outside vendors can also be fined or banned if they break the rules.

**(f) *Emergencies & Exceptions***

- (i) In emergencies, employees can use new AI tools, but only if they get approval from the IT Director and the City Administrator.



# Artificial Intelligence (AI) Policy

## 1. Purpose

- 1.1. This policy explains how the City of Dripping Springs will use Artificial Intelligence (AI) tools in a safe and responsible way. It sets up rules and guidance to help city staff use AI to improve services while protecting people from harm.
- 1.2. The main goals are to:
  - (a) Give clear instructions to staff who buy, set up, use, or manage AI tools.
  - (b) Make sure AI tools follow important values like safety, fairness, and transparency.
  - (c) Clarify who is responsible for what when it comes to using AI.
  - (d) Create a process to check for risks and benefits of using AI.
  - (e) List what kinds of AI use are not allowed.
  - (f) Make sure AI is only used for real City business and follows all laws and policies.

## 2. Terms & Definitions

- 2.1. **Artificial Intelligence** or **AI**: A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.<sup>1</sup> AI systems can make predictions, give advice, or make decisions based on goals set by people. It uses data to understand situations and suggest actions.
- 2.2. **Algorithm**: A set of instructions a computer follows to turn input (like data) into output (like answers or actions).

---

<sup>1</sup> Definition from [15 U.S.C. 9401\(3\)](#).

- 2.3. **AI system:** Has the same meaning as defined under Section 2054.003(1-a) of the Texas Government Code, as amended. (i.e., “A machine-based system that for explicit or implicit objectives infers from provided information a method to generate outputs, such as predictions, content, recommendations, or decisions, to influence a physical or virtual environment with varying levels of autonomy and adaptiveness after deployment.”)
- 2.4. **Cognitive behavioral manipulation:** AI-driven tools or algorithms designed to influence or alter an individual’s decision-making process or belief system. These systems use psychological, behavioral, or emotional data to create targeted strategies that can manipulate thoughts, feelings, or actions, particularly focusing on vulnerable groups or individuals.
- 2.5. **Consequential decision:** Has the same meaning as defined under Section 2054.003(2-b) of the Texas Government Code, as amended. (i.e., “means a decision that has a material legal or similarly significant effect on the provision, denial, or conditions of a person’s access to a government service.”)
- 2.6. **Controlling factor:** Has the same meaning as defined under Section 2054.003(2-c) of the Texas Government Code, as amended. (i.e., “means a factor that is: (A) the principal basis for making a consequential decision; or (B) capable of altering the outcome of a consequential decision.”). If AI is the main reason for a decision, it’s considered a controlling factor.
- 2.7. **DIR:** The Texas Department of Information Resources.
- 2.8. **DIR Artificial Intelligence System Code of Ethics:** A set of rules from DIR that guides how government agencies should use AI responsibly, s developed by DIR pursuant to Section 2054.702 of the Government Code, as amended.
- 2.9. **DIR Minimum Standards for Heightened-Scrutiny AI Systems:** Extra rules for AI systems that make important decisions on their own. These rules help manage risks and ensure safety, developed by DIR pursuant to Section 2054.703 of the Government Code, as amended.
- 2.10. **Heightened-scrutiny AI system:** An AI system that makes big decisions without human help. These systems need extra review and approval. It is defined under Section 2054.003(6-a) of the Texas Government Code as “ an artificial intelligence system specifically intended to autonomously make, or be a controlling factor in making, a consequential decision. The term does not include an artificial intelligence system intended to:
- (a) perform a narrow procedural task;
  - (b) improve the result of a previously completed human activity;
  - (c) perform a preparatory task to an assessment relevant to a consequential decision; or

- (d) detect decision-making patterns or deviations from previous decision-making patterns.”)

2.11. **NIST:** National Institute of Standards and Technology.

2.12. **Personally Identifiable Information** or **PII:** Any information that can identify a person, like their name plus:

- (e) Social Security number
- (f) Driver’s license or ID
- (g) Passport number
- (h) Credit card info
- (i) Phone number
- (j) Birthdate
- (k) Medical records
- (l) Biometric data (like fingerprints)
- (m) Home address or email
- (n) IP address
- (o) And more

2.13. **Principal basis:** When a decision is made mostly because of what the AI says, without a person reviewing or questioning it. It is defined under section 2054.003(11) of the Texas Government Code, as “the use of an output produced by a heightened scrutiny artificial intelligence system to make a decision without: (A) human review, oversight, involvement, or intervention; or (B) meaningful consideration by a human.”

### 3. Scope

This policy applies to:

- (a) All AI systems that the City of Dripping Springs uses, buys, builds, or manages.
- (b) Anyone working for the City—including full-time and part-time staff, interns, and volunteers—who uses or manages AI systems or data.
- (c) Any AI system used to provide services for the City, even if it's operated by someone outside the City.

## 4. Guiding Principles for Responsible AI Systems

- 4.1. The City adopts and will maintain conformance with the DIR Artificial Intelligence System Code of Ethics developed under Section 2054.702 of the Texas Government Code and DIR Minimum Standards for Heightened-Scrutiny AI Systems, which align to [NIST Artificial Intelligence Risk Management Framework \(AI RMF 1.0\)](#)
- 4.2. **Human-Centered Design:** AI should be built and used in ways that focus on people's needs and impacts.
- 4.3. **Security & Safety:** AI systems must be protected from misuse. They should be reliable and not put people, the community, or the environment at risk.
- 4.4. **Privacy:** AI must protect personal and sensitive information. This includes things like names, addresses, medical records, and other private data. Privacy is preserved in all AI systems by safeguarding personally identifiable information (PII) and sensitive data from unauthorized access, disclosure, and manipulation as defined in this policy. City information that must be kept private can include both PII and sensitive data as well as information that would be released if requested under the Public Information Act.
- 4.5. **Transparency:** The City will clearly explain how and why AI is used—unless the law says otherwise. People should be able to understand what the AI does and how it works.
- 4.6. **Accountability:** People, not machines, are responsible for how AI is used. There must be clear roles and oversight to make sure rules are followed.
- 4.7. **Effectiveness:** AI systems are reliable, meet their objectives, and deliver precise and dependable outcomes for the utility and contexts in which they are used.
- 4.8. **Workforce Empowerment:** City staff will be trained and supported to use AI tools in their jobs.

## 5. AI Governance Framework: Management, Oversight, and Accountability.

This section explains who is responsible for making sure AI is used properly in the City of Dripping Springs.

- 5.1. **City Council & City Administrator:** They oversee how AI is used and make final decisions.
- 5.2. **IT Director:**
  - (a) Manages all City technology and AI tools.
  - (b) Reviews and approves AI systems, especially those that make important decisions, pursuant to Section 2054.0965(c) of the Texas Government Code.



- (c) Keeps a list of approved and banned AI tools.
- (d) Makes sure AI use follows City policies and laws.
- (e) Handles cybersecurity and digital privacy.
- (f) Updates security rules and checks for compliance.
- (g) Coordinates with other departments and updates policies when needed.
- (h) Coordinates with the Human Resources Director to notify City staff when this policy changes.
- (i) Coordinates with the People and Communications Director to ensure public-facing AI tools include proper notices.

**5.3. City Attorney's Office:**

- (a) Adds rules to contracts to make sure vendors follow safety standards.
- (b) Advises the City on legal risks related to AI.

**5.4. Department Heads:**

- (a) Identify which employees use computers for at least 25% of their job.
- (b) Make sure those employees complete yearly AI and cybersecurity training.

**5.5. City Administrator**

- (a) Identifies officials who need AI training.
- (b) Can inspect how AI is used and stop or change its use if needed.

**5.6. People & Communications Director**

- (a) Makes sure the City's website includes a link to report AI-related complaints.
- (b) Verifies that public-facing AI tools have proper notices.

**6. Prohibited Uses**

- 6.1. Some uses of AI are not allowed because they can be harmful, unfair, or unsafe. If you think an AI system has caused harm, report it right away to your supervisor and the IT Director, and file a written report.

6.2. The City does NOT allow:

- (a) Using any AI tool that hasn't been approved by the IT Director. (See Appendix A).
- (b) Using any AI tool listed as banned in Appendix B.
- (c) AI that gives people a score or ranking that affects their access to services or opportunities.
- (d) AI that makes important decisions without a person reviewing or approving it.
- (e) AI that tracks or judges people based on behavior, income, or personal traits (social scoring).
- (f) AI that uses photos or videos from the internet to identify people without their permission.
- (g) AI that encourages self-harm, violence, or illegal activity.
- (h) Putting personal or private City information into AI tools that are not part of the City's secure systems (like cloud-based AI).
- (i) Sharing confidential City information with AI tools that are not approved or secure.
- (j) Using AI tools to share City information that hasn't been made public or has been restricted by City leadership.
- (k) AI assistants or features that automatically summarize, read, or interact with City email accounts or email content
- (l) AI-powered browsers or browser features (such as Atlas from ChatGPT, or AI browsing modes in Edge, Chrome, etc.). This includes any browser or extension that uses AI to interact with, summarize, or automate tasks within web sessions.

## 7. Public-Facing AI

- 7.1. If the City uses AI tools that interact directly with the public, such as on websites, kiosks, or forms, it must clearly tell people that AI is being used.
- 7.2. A clear and easy-to-understand notice must be shown to users before or during their first interaction with the AI.

- 7.3. The notice must follow rules set by the Texas Department of Information Resources (DIR).

## **8. Public Records**

The City of Dripping Springs must follow the Texas Public Information Act. This means:

- (a) All records, including those created using AI, must be saved and managed properly.
- (b) City employees must follow current rules for keeping and sharing records.
- (c) If you have questions about public records, ask the City Secretary or the City Attorney's Office.

## **9. Training**

Every year, certain City staff and officials must complete certified AI training by a deadline set by state law.<sup>2</sup> This includes:

- (a) Anyone who uses a computer for at least 25% of their job.
- (b) Any other employee or volunteer the City Administrator requires to take the training.

## **10. Violations of the AI Policy**

- 10.1. Breaking any part of this AI Policy can lead to serious consequences.
- 10.2. Violations by City employees may result in disciplinary action, including possible termination.
- 10.3. Violations by outside vendors or contractors may be considered a breach of contract. They may face fines, legal actions, or be banned from working with the City.
- 10.4. If laws are broken, the issue may be reported to law enforcement or other government agencies.

## **11. Exceptions**

- 11.1. If you need to use an AI tool in a way that's not allowed, you must get written approval from the IT Director or City Administrator. If you don't have formal approval, it will be treated as a security issue.

---

<sup>2</sup> Tex. Gov't. Code, § 2054.5191.

- 11.2. In urgent situations, staff may use new AI tools, but only after getting documented approval from the IT Director. Each emergency use must be reviewed and approved before the tool is used.

## **12. Preemption and Construction**

- 12.1. This policy should be interpreted in line with Texas state laws, especially the Texas Government Code and the Texas Business and Commerce Code.
- 12.2. If there's ever a conflict between this policy and state law, the state law will take priority.

# Appendix A:

## Permitted AI Platforms

The following is a list of AI platforms that have been approved for use by the City of Dripping Springs. Use of any unlisted AI tool requires prior IT approval and a completed risk assessment.

If a platform is not on this list that an employee would like to use, the employee must complete an AI Approval Request Form (see [Appendix C](#)) and submit it to the IT Director for review. Please keep in mind that some AI platforms have multiple names or subsidiaries. When in doubt whether a platform or program has been approved, please contact the IT Director:

AI Platform	Creator/Owner	Description
<b>Chat GPT</b>	OpenAI	Helps with questions, writing, brainstorming, programming, and productivity
<b>CoPilot</b>	Microsoft	Productivity assistance, data analysis, email management, meeting summaries, task automation
<b>Grok</b>	xAI	Primarily used for summarizing live trends, crafting social media content, coding help, and multimodal interaction
<b>Gemini</b>	Google	Enhances search and productivity across Google apps and services; Assists w/ code writing and research automation; supports conversational voice and visual interaction for everyday tasks; provides document- synthesis tools; integrates into workflows
<b>Claude.ai</b>	Anthropic	Facilitates writing, summarization, and research; assists w/ code generation and debugging; performs deep reasoning and handles large-context tasks; operates with a constitutional AI architecture to ensure safety, transparency, and ethical responses

# Appendix B:

## Prohibited AI Platforms

The following platforms, tools, and features are explicitly prohibited absent written approval from the IT Director. Use of any unlisted AI tool requires prior IT approval and a completed risk assessment. This prohibition includes, but is not limited to:

AI assistants that access, read, summarize, or otherwise interact with City email accounts or email content (e.g., Gemini for Gmail, Copilot email summarization, or similar features).

AI-powered browsers, browser modes, or extensions that use AI to interact with, summarize, or automate web sessions (e.g., Atlas from ChatGPT, AI modes in Edge/Chrome, or similar).~~The following is a list of AI platforms that is explicitly prohibited. Use of any unlisted AI tool requires prior IT approval and a completed risk assessment. Please keep in mind that some AI platforms have multiple names or subsidiaries. When in doubt whether a platform or program has been approved, please contact the IT Director.~~

If a platform appears on this list and usage is desired please reach out to the IT department.

[Note: The IT Director may add or remove specific tools from Appendix B via administrative update.]

AI Platform	Creator/Owner
Deepseek	Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co.

# Appendix C:

## AI Approval Request Form

*Submit this form to the IT Director before purchasing, configuring, using, or materially changing any AI system used for City business.*

### A. Request Summary

1. **Requester name & title:** Click or tap here to enter text.
2. **Department:** Click or tap here to enter text.
3. **Date:** Click or tap to enter a date.
4. **Type of request (check all that apply):**
  - ☐ New AI tool
  - ☐ Renewal/extension
  - ☐ Material change (new data, new feature, new use)
  - ☐ Pilot/trial
  - ☐ Emergency/exception (complete Section I)
5. **Brief description of the AI use case (2–3 sentences):**  
Click or tap here to enter text.
6. **Intended go-live date:** Click or tap to enter a date.

### B. AI System Details

1. **AI platform/product name:** Click or tap here to enter text.
2. **Vendor/Creator (legal entity):** Click or tap here to enter text.
3. **Product URL:** Click or tap here to enter text.
4. **Version/plan:** Click or tap here to enter text.

**5. Deployment model:**

- ☐ SaaS (cloud)
- ☐ On-premises
- ☐ Hybrid

**6. Is this platform listed in Appendix A (Permitted AI Platforms)?**

- ☐ Yes
- ☐ No

**7. Is this platform listed in Appendix B (Prohibited AI Platforms)?**

- ☐ Yes → Stop. Do not proceed.
- ☐ No

**8. Will the system be public-facing (e.g., website, kiosk, form/chat for residents)?**

- ☐ Yes (complete Section F re: standardized notices)
- ☐ No

**9. Will the system autonomously make, or be a controlling factor in making, a consequential decision?**

- ☐ Yes (This is a Heightened Scrutiny AI. Complete Section E in full)
- ☐ No

**10. Primary purpose/benefits (select all):**

- ☐ Drafting/summarization
- ☐ Forecasting/scoring
- ☐ Classification/routing
- ☐ Image/audio/video processing
- ☐ Search/retrieval
- ☐ Code assistance/automation
- ☐ Other: Click or tap here to enter text.

**11. City business functions supported: Click or tap here to enter text.**

**12. Expected frequency/volume of use: Click or tap here to enter text.**



## C. Data & Privacy

### 1. Data categories involved (check all that apply):

- |   |  |
|---|--|
| <input type="checkbox"/> Public records / general administrative data | <input type="checkbox"/> Health/medical  |
| <input type="checkbox"/> Personal Identifiable Information (PII)      | <input type="checkbox"/> Biometric   |
| <input type="checkbox"/> Confidential City information (non-public)   | <input type="checkbox"/> Location data / identifiers (e.g., plates, IPs)           |
| <input type="checkbox"/> Financial/PCI                                | <input type="checkbox"/> Images/audio/video  |
| <input type="checkbox"/> Personnel data                               | <input type="checkbox"/> Other sensitive data:<br>Click or tap here to enter text. |

*PII list per policy includes (non-exhaustive): SSN, DL/ID, passport, credit/debit details, account numbers, DOB, mother's maiden name, PINs/passwords, tax status, biometrics, signatures, personal contact details, medical data, vehicle identifiers, insurance policy numbers, IP addresses, etc.*

### 2. Will any PII or confidential City information be entered into a cloud-hosted AI outside City-secured systems?

- |  |   |
|--|---|
| <input type="checkbox"/> No (required) | <input type="checkbox"/> Yes → <b><u>Prohibited by policy.</u></b><br><b><u>Do not proceed.</u></b> |
|--|---|

### 3. Data sources (systems/files) the AI will access:

#### (a) Data flow summary:

- (i) *Inputs provided to AI:* Click or tap here to enter text.
- (ii) *Outputs produced by AI:* Click or tap here to enter text.
- (iii) *Where outputs are stored (system/location):* Click or tap here to enter text.
- (iv) *Retention period & records classification:* Click or tap here to enter text.

#### (b) Access controls:

- (i) *Who can use the tool:* Click or tap here to enter text.
- (ii) *Who can see inputs/outputs:* Click or tap here to enter text.

- (iii) *Authentication/SSO:* *Click or tap here to enter text.*
- (c) Public Information Act compliance plan:
- (i) *How related records (prompts, outputs, configurations, logs) will be retained and produced upon request: Click or tap here to enter text.*

## **D. Effectiveness, Safety & Security**

1. **Human oversight (“human-in-the-loop”) – Describe how staff will review/validate AI outputs.**  
*Click or tap here to enter text.*
2. **Testing & evaluation – Describe how accuracy, bias, and error rates will be measured before and after use; include acceptance criteria.**  
*Click or tap here to enter text.*
3. **Security – Describe protections (e.g., encryption at rest/in transit, admin controls, logging, audit trails, vendor SOC 2/ISO 27001).**  
*Click or tap here to enter text.*
4. **Confirmed Incident reporting – You will report suspected harm, misuse, or policy violations to your supervisor and the IT Director immediately, with a written incident report. ☐**
5. **Confirmed Training – Identify who must complete annual AI training (employees/officials using a computer  $\geq 25\%$  of duties) and confirm training is/will be completed. ☐**  
*Click or tap here to enter text.*

## **E. Heightened-Scrutiny AI (complete if “Yes” in Section B)**

1. **Consequential decision(s) impacted:** *Click or tap here to enter text.*
2. **Is the AI a controlling factor?**  
☐ Yes ☐ No
3. **Safeguards for meaningful human review (not rubber-stamping):**  
*Click or tap here to enter text.*
4. **Notice plan – Link/location of standardized notice on apps/websites/public systems:**  
*Click or tap here to enter text.*

**5. Risk management alignment:**

- (a) DIR AI System Code of Ethics: ☐ Aligns
- (b) DIR Minimum Standards for Heightened-Scrutiny AI: ☐ Aligns
- (c) NIST AI RMF (Map, Measure, Manage, Govern): ☐ Addressed
- 6. Appeal/contest process for affected individuals:**  
Click or tap here to enter text.

**F. Public-Facing AI (if applicable)**

- 1. Plain-language disclosure – Provide the exact text that will be shown to users before/at first interaction and where it will appear.**  
Click or tap here to enter text.
- 2. Standardized notice – Provide link showing the required notice on all relevant systems.**  
Click or tap here to enter text.
- 3. Accessibility & language access – Describe how notices/interactions meet accessibility and language needs.**  
Click or tap here to enter text.

**G. Alternatives & Justification**

- 1. Alternatives considered (including non-AI options) and why they were not selected:**  
Click or tap here to enter text.
- 2. Expected benefits vs. risks/costs (staff time, accuracy, public trust, security):**  
Click or tap here to enter text.
- 3. Success metrics/KPIs:** Click or tap here to enter text.

**H. Procurement & Contracting (attach draft agreement, SOW, or terms)**

- 1. Contract includes vendor obligations to implement a risk-management framework consistent with DIR Minimum Standards for Heightened-Scrutiny AI (Gov't Code §2054.703(b)(4)(B)).** ☐
- 2. Data processing & confidentiality terms (no training on City data without explicit consent; data residency; deletion/export on termination).** ☐

3. Security & compliance (SOC 2/ISO 27001; breach notification; audit rights). ☐
4. Records retention & e-discovery cooperation. ☐
5. Price/term & termination for convenience. ☐
6. Prohibition on social scoring, fully automated consequential decisions, biometric scraping, or other prohibited uses. ☐
7. If subscription/SaaS:
  - (a) Tenant isolation details: [Click or tap here to enter text.](#)
  - (b) Opt-out of model training on prompts/outputs: ☐

## **I. Emergency/Exception Request**

(complete only if claiming emergency or seeking exception)

1. Emergency circumstance & public interest rationale:  
[Click or tap here to enter text.](#)
2. Duration of temporary use: [Click or tap here to enter text.](#)
3. Safeguards to mitigate risk during emergency use:  
[Click or tap here to enter text.](#)

## **J. Inventory & Compliance (for IT Director to complete)**

1. AI system category (regular / heightened-scrutiny):  
[Click or tap here to enter text.](#)
2. Controlling factor in consequential decision? ☐ Yes ☐ No
3. Datasets used: [Click or tap here to enter text.](#)
4. Vendor & contact: [Click or tap here to enter text.](#)
5. Purpose/department: [Click or tap here to enter text.](#)
6. Assessment date(s): [Click or tap to enter a date.](#)
7. Standardized-notice URL/location: [Click or tap here to enter text.](#)
8. System owner (department lead): [Click or tap here to enter text.](#)

9. **Review due date (annual):** Click or tap to enter a date.

## **K. Approvals**

**1. Department Head**

Name/Title: \_\_\_\_\_

Signature/Date: \_\_\_\_\_ / \_\_\_\_\_

**2. IT Director ☐ Approved ☐ Denied**

Notes/conditions:

Signature/Date: \_\_\_\_\_ / \_\_\_\_\_

**3. City Attorney (Legal review complete ☐ Yes)**

Name/Title: \_\_\_\_\_

Signature/Date: \_\_\_\_\_ / \_\_\_\_\_

**4. People & Communications Director (for public-facing AI) – Disclosure/notice verified ☐ Yes**

Name/Title: \_\_\_\_\_

Signature/Date: \_\_\_\_\_ / \_\_\_\_\_

**5. City Administrator ☐ Approved ☐ Denied**

Conditions: Click or tap here to enter text.

Signature/Date: \_\_\_\_\_ / \_\_\_\_\_

## **L. Attachments Checklist**

- ☐ Product description/one-pager
- ☐ Security/Privacy documentation (SOC 2/ISO 27001, DPAs)
- ☐ Data flow diagram
- ☐ Testing/validation plan & results
- ☐ Notice text/screenshots (if public-facing or controlling factor)
- ☐ Draft contract/SOW/terms

- ☐ Training plan/roster
- ☐ Records retention plan
- ☐ Any additional assessments (bias, accessibility, impact)

## **M. Policy Reminders (for requesters)**

- Do not input PII or confidential City information into cloud AI outside City-secured systems.
- Prohibited uses include social scoring; fully automated consequential decisions without meaningful human oversight; biometric ID using scraped/public images; and AI aimed at self-harm/violence.
- Public-facing or controlling-factor systems must include standardized notices; affected individuals must have a way to appeal.
- Annual AI training is required for applicable staff and officials.
- All AI-related records (prompts, outputs, configs, logs) are subject to retention and disclosure under the Texas Public Information Act.