

CITY OF MISSION, TEXAS**ARTIFICIAL INTELLIGENCE GOVERNANCE AND
ACCEPTABLE USE POLICY***Effective Date: Upon approval***1. Purpose and Scope**

The City of Mission encourages the responsible use of artificial intelligence to improve employee productivity, municipal operations, analysis, public communication, service delivery, and innovation.

This Policy establishes practical requirements for the use of AI while protecting City information, maintaining human accountability, and complying with applicable state and federal law.

This Policy applies to City employees, elected and appointed officials, interns, and volunteers conducting City business.

Contractors, consultants, and vendors are subject to applicable AI requirements established through their contracts, their access to City information or systems, and applicable law.

2. Governing State Standards

The City adopts and incorporates by reference the Texas Department of Information Resources (DIR) Artificial Intelligence Code of Ethics and applicable minimum standards established pursuant to:

- Texas Government Code §§2054.702–2054.703;
- Texas Government Code Chapter 2054, Subchapter S;
- 1 Texas Administrative Code Chapter 219; and
- Applicable provisions of the Texas Responsible Artificial Intelligence Governance Act (TRAIGA), Texas Business & Commerce Code Chapter 552.

These requirements, including future amendments, successor provisions, and implementing rules, are incorporated into this Policy to the extent applicable to the City.

State and federal law shall control if a provision of this Policy conflicts with applicable law.

The City Manager or designee may update administrative procedures, approved-tool lists, forms, and implementation guidance as necessary to remain consistent with changes in applicable law or DIR standards.

3. Key Definitions

The following definitions are intended to help employees recognize the type of information and AI use involved before using an AI system.

Artificial Intelligence System

A machine-based system that uses information to generate outputs such as content, predictions, recommendations, or decisions with varying levels of autonomy.

Public or General-Purpose AI System

A commercial or internet-accessible AI system that is not specifically approved by the City to process protected City information.

This may include consumer versions of general-purpose AI chatbots and other web-based AI services.

City-Approved Secure AI System

An AI-enabled system that has been reviewed and specifically authorized by the City for the information and purpose involved.

Approval for one type of information does not mean the system is approved for all City information.

Personally Identifiable Information (PII)

Information that, by itself or when combined with other information, identifies or can reasonably identify a particular individual.

PII can include:

- A person's name when connected to nonpublic or sensitive information;
- Home address;
- Personal telephone number or personal email address;
- Date of birth;
- Social Security number;
- Driver's license, state identification, or passport number;
- Employee, customer, patient, utility, account, or case number;
- Personal financial account or payment information;
- Medical or health information;
- Biometric information;
- Precise personal location information; or
- A combination of facts that would reasonably allow a person to be identified.

Information is not automatically confidential merely because it identifies a person. Names, titles, salaries, vendor information, contract information, public project addresses, public accounting records, and other information lawfully available to the public may generally be used when appropriate for the City purpose involved and when no separate confidentiality requirement applies.

Appropriately Anonymized Information

Information is appropriately anonymized when identifying information has been removed, masked, generalized, or replaced so that an individual cannot reasonably be identified from the remaining information, either alone or when combined with other reasonably available information.

Consequential Decision

A Consequential Decision, as defined by Texas Government Code §2054.003, is a decision having a material, legal, or similarly significant effect on the provision, denial, or conditions of a person's access to a government service.

Depending on the system and how it is used, examples may include decisions concerning:

- Eligibility for a City program or service;
- Approval or denial of assistance or benefits;
- Connection, continuation, restriction, or denial of a City service;
- Approval, denial, or material conditions of a permit or license; or

- Another City decision materially affecting a person's access to governmental services.

Controlling Factor

An AI output is a Controlling Factor when it is the principal basis for making a Consequential Decision or when the AI output is capable of changing the outcome of that decision.

An AI system does not avoid this classification merely because an employee performs a final administrative approval if the AI result effectively determines or can materially change the outcome.

Heightened Scrutiny AI

A Heightened Scrutiny AI System is an AI system specifically intended to:

1. Autonomously make a Consequential Decision; or
2. Serve as a Controlling Factor in making a Consequential Decision.

Under Texas law, the term does not include an AI system intended only to:

- Perform a narrow procedural task;
- Improve the result of a previously completed human activity;
- Perform a preparatory task for an assessment relevant to a Consequential Decision; or
- Detect decision-making patterns or deviations from previous decision-making patterns.

4. Permitted AI Use and Information Protection

Employees may use AI tools permitted by Information Technology for legitimate City business, including:

- Drafting and editing;
- Research and summarization;
- Presentations and training materials;
- Translation;
- Spreadsheet formulas;
- Data and trend analysis;
- Accounting, budget, and financial analysis;
- Operational reporting;
- Planning;
- Process improvement;
- Document organization; and
- Other appropriate municipal activities.

Public information and appropriately anonymized information may be processed through permitted general-purpose AI tools.

Employees remain responsible for reviewing and verifying the resulting work.

Information That Should Be Removed or Anonymized

Before providing a City report, spreadsheet, document, or dataset to a general-purpose AI system, employees shall review the information and remove or anonymize nonpublic identifying information that is not necessary for the task.

This generally includes:

- Names connected to confidential customer, patient, personnel, complaint, investigation, or case information;
- Personal residential addresses when they are not already public and necessary for the work;

- Personal telephone numbers and personal email addresses;
- Dates of birth;
- Social Security numbers;
- Driver's license, identification, or passport numbers;
- Employee, patient, utility customer, case, or other unique identification numbers;
- Bank account, routing, payment card, login, or authentication information;
- Protected health or medical information;
- Confidential personnel information;
- Biometric identifiers;
- Precise personal location information; and
- Other combinations of information that could reasonably identify an individual in a nonpublic matter.

Employees should also remove fields that are unnecessary for the analysis even when those fields are not independently confidential. This practice reduces unnecessary disclosure of personal information.

Employees may replace identifiers with neutral labels such as **Resident A**, **Employee 1**, **Account A**, or another non-identifying reference when the identity of the person is not necessary for the analysis.

Public Information Does Not Require Automatic Redaction

Information does not need to be anonymized solely because it contains a name or address if the information is lawfully public, appropriate for the City purpose involved, and not subject to another confidentiality restriction.

Examples may include:

- Names and titles of City officials and employees contained in public records;
- Public salary and compensation information;
- Vendor and contractor names;
- Public contracts and expenditures;
- City facility addresses;
- Public project or construction information;
- Publicly released budgets and financial statements; and
- Other information already lawfully available to the public.

If an employee is uncertain whether information is public, protected, or sufficiently anonymized, the employee should consult the **AI Risk Officer or Information Technology Director** before submitting the information to an AI system.

Approved Secure AI Systems

Protected information may be processed through an AI system only when that system has been specifically reviewed and approved for that category of information and purpose.

Before approval, the review shall consider:

- Privacy requirements;
- Cybersecurity requirements;
- Access controls;
- Records retention and data deletion;
- Contractual protections; and
- Applicable legal requirements.

Approval of a specialized system does not authorize employees to place the same protected information into a general-purpose or otherwise unapproved AI system.

5. Human Oversight and Responsible Use

Employees remain responsible for their final work product and for decisions made in the course of their City duties.

Material AI-generated information shall be reviewed and verified as appropriate, including:

- Facts;
- Calculations;
- Citations;
- Legal references;
- Financial figures;
- Dates;
- Names; and
- Other significant information.

The level of human review should increase with the significance of the activity and potential consequences of an error.

AI shall not replace professional judgment where professional, legal, medical, engineering, accounting, public-safety, or other specialized judgment is required.

AI shall not be used to:

- Fabricate official information, evidence, records, or citations;
- Impersonate City personnel;
- Create intentionally deceptive content;
- Unlawfully discriminate;
- Circumvent cybersecurity or access controls;
- Override required human approval; or
- Represent unverified AI output as independently established fact.

6. Identifying and Reviewing Higher-Risk AI Systems

Departments are responsible for recognizing when a proposed AI system may go beyond ordinary employee productivity assistance and may affect a Consequential Decision.

When a Department Must Consult the AI Risk Officer and IT Director

Before developing, procuring, implementing, or using an AI system, a department shall contact the **AI Risk Officer and Information Technology Director** when the system may:

- Automatically approve, deny, or condition access to a City service;
- Generate a score, classification, recommendation, or determination that could change the outcome of a Consequential Decision;
- Serve as the principal basis for a decision affecting access to a City service;
- Automatically make a decision that would otherwise be made by City personnel;
- Process protected information as part of a significant decision-making system; or
- Otherwise reasonably appear to meet the definition of Heightened Scrutiny AI.

Departments are encouraged to consult the AI Risk Officer and IT Director **before procurement or use whenever classification is uncertain.**

No employee or department is expected to independently make a final legal determination that a system qualifies as Heightened Scrutiny AI. The purpose of the referral is to allow the AI Risk Officer and appropriate City personnel to make that assessment before the City becomes committed to the technology.

7. AI Risk Officer and DIR Requirements for Heightened Scrutiny AI

The City Manager shall designate an employee to serve as the **AI Risk Officer**, as required by 1 Texas Administrative Code §219.21.

The AI Risk Officer shall coordinate with the Information Technology Director and relevant departments to promote ethical AI procurement, development, deployment, and use and to administer the City's process for identifying and inventorying Heightened Scrutiny AI systems.

Required Review

When a proposed system qualifies as Heightened Scrutiny AI, the following requirements shall be completed before the City develops, procures, deploys, or uses the system and again when a material change is made.

Written AI Risk Assessment

A written risk assessment shall evaluate the probability and severity of potential harm and shall document, at minimum:

1. Security

- Known security risks; and
- Available mitigation measures.

2. Performance

- Accuracy-related performance measures; and
- Operational-efficiency measures appropriate to the system.

3. Transparency

- Available information concerning the system's algorithms and how decisions are generated;
- The data used to train the system's model; and
- Whether system inputs and outputs are available for monitoring decision-making over time.

AI Risk Officer Determination

Before deployment, the AI Risk Officer shall:

- Review the completed written risk assessment;
- Evaluate identified risks and mitigation measures;
- Approve or deny deployment of the system; and
- Notify the City Manager or designee of a decision to deploy the system.

The City shall retain the completed assessment and related documentation in accordance with applicable records-retention requirements.

System-Specific Requirements

For each Heightened Scrutiny AI system deployed or used by the City, the City shall:

- Identify the approved use cases for the system;
- Identify the system's known limitations;
- Establish system-specific acceptable-use requirements preventing unauthorized uses;
- Train employees on those acceptable-use requirements;

- Provide employees and contractors who access, use, or manage the system training concerning identified risks and methods for reducing those risks; and
- Require applicable vendors to maintain an AI risk-management framework consistent with the NIST AI Risk Management Framework or another comparable standard.

The AI Risk Officer shall also consider whether an AI impact assessment aligned with applicable DIR guidance is appropriate for a proposed Heightened Scrutiny AI system and shall review relevant resources published by DIR.

8. Public Disclosure, Notice, and Redress

The City shall comply with applicable public-disclosure requirements established by TRAIGA, Texas Government Code Chapter 2054, and DIR.

Public-Facing AI

When the City provides an AI system intended to interact directly with members of the public, the City shall provide the disclosure required by TRAIGA before or at the time the interaction begins.

The disclosure shall be clear and conspicuous and shall comply with applicable state requirements.

DIR Standardized Notice

The City shall use the standardized notice prescribed by DIR when the City deploys or uses an AI system that:

- Is public-facing; or
- Serves as a Controlling Factor in a Consequential Decision.

As required by Texas Government Code §2054.711, the applicable standardized notice shall be included on related applications, City websites, and public computer systems.

Applicable healthcare-related AI systems shall also comply with any additional disclosure requirements imposed by law.

Public Contact and Redress

The City shall maintain a designated point of contact for individuals seeking information concerning an allegedly unfair AI-assisted Consequential Decision.

A general City email address, online form, or other designated contact method may serve as the point of contact.

The City shall maintain a mechanism through which individuals may seek redress when an AI system makes a Consequential Decision resulting in unlawful harm affecting the person's rights or access to governmental services.

The City Manager or designee shall establish internal procedures for reviewing, routing, and addressing those requests.

9. AI Incident Reporting

Employees shall immediately notify both the **AI Risk Officer and Information Technology Director** upon discovering or reasonably suspecting:

- Unauthorized disclosure of protected information through an AI system;
- Significant AI-related security concerns;

- Unauthorized access to an AI system;
- Material AI errors affecting City operations or services; or
- Other significant AI-related incidents.

The affected department shall follow the City's existing cybersecurity, privacy, records, legal, or other applicable incident-response procedures.

Incidents involving specialized information, including protected health information, shall also follow the applicable departmental and legal reporting process.

Detailed investigation, containment, notification, and management-response procedures may be maintained separately by the responsible City departments.

10. Records Management, Procurement, and Vendors

Records Management

AI-assisted City work remains subject to applicable public-information and records-retention requirements.

Employees shall retain official City records in approved City systems.

AI prompts, inputs, outputs, transcripts, assessments, or related materials shall be retained or preserved when required by:

- Applicable records-retention schedules;
- The Texas Public Information Act;
- A legal hold;
- Litigation;
- An audit;
- An investigation; or
- Another applicable preservation requirement.

Departments deploying AI systems shall consider the Public Information Act and records-retention implications of storing system inputs and outputs.

Procurement and Vendors

Before procuring or implementing an AI system that processes protected information, performs a significant City function, or otherwise requires City approval, the requesting department shall review the proposed system with the **Information Technology Director and AI Risk Officer**.

The review shall evaluate, as applicable:

- Privacy;
- Cybersecurity;
- Vendor data use;
- Data ownership;
- Access controls;
- Reliability and accuracy;
- Data retention and deletion;
- Vendor training or reuse of City data;
- Contractual safeguards; and
- Applicable state and federal requirements.

A **written approval memorandum** documenting the review and approval of both the Information Technology Director and AI Risk Officer shall be completed before procurement or implementation of the system.

Contracts involving material AI functionality shall contain safeguards appropriate to the information and service involved.

Vendors supporting Heightened Scrutiny AI shall comply with the additional requirements established by DIR and this Policy.

11. AI Training

The City will maintain both **state-required AI awareness training** and **City practical AI-use training**.

DIR-Certified AI Awareness Training

Employees and officials meeting the criteria established by Texas Government Code §2054.5191 shall complete a DIR-certified AI awareness training program annually.

The City shall document completion and complete applicable reporting to DIR.

City AI Practical Training

Employees authorized to use AI for City business shall receive City-provided practical training sufficient to understand how to use AI effectively and responsibly, how to navigate and comply with this Policy, and when to seek assistance from the AI Risk Officer or Information Technology.

The City may provide additional role-based training for departments or employees using specialized AI systems.

Employees and contractors who access, use, or manage Heightened Scrutiny AI shall receive the additional system-specific training required by DIR.

12. Evaluation and Administration

The AI Risk Officer and Information Technology shall establish methods for the regular evaluation of AI systems to ensure they continue to provide appropriate benefit and operate consistently with applicable requirements.

The City shall document those evaluations as required by the DIR Artificial Intelligence Code of Ethics.

The City Manager or designee may issue and revise supporting administrative procedures and implementation materials without amending this Policy unless formal approval is otherwise required.

13. Governing References

Texas Government Code Chapter 2054, Subchapter S

Artificial Intelligence requirements applicable to governmental entities.

Texas Government Code §§2054.702–2054.703

DIR Artificial Intelligence Code of Ethics and minimum standards.

Texas Government Code §2054.711

Standardized AI notice requirements.

Texas Government Code §2054.5191

Annual artificial intelligence awareness training requirements.

1 Texas Administrative Code Chapter 219

DIR Artificial Intelligence Code of Ethics, AI Risk Officer requirements, Heightened Scrutiny AI risk assessments, acceptable-use requirements, training, and vendor risk-management requirements.

Texas Business & Commerce Code Chapter 552

Texas Responsible Artificial Intelligence Governance Act (TRAIGA).

Texas Government Code Chapter 552

Texas Public Information Act.

Applicable federal and state privacy, healthcare, cybersecurity, records-retention, employment, civil-rights, accessibility, procurement, and professional requirements.