ARLINGTON℠
THE AMERICAN DREAM CITY

Generative AI Security Policy

A. DOCUMENT AND INFORMATION HISTORY

Publication Information

Scope	Citywide
Authorized By	City Manager’s Office
Review Frequency	Annually
Supersedes	N/A

Publication Version History

Numbering convention: Version as n.x. Pre-publication drafts are 0.x; first published version is 1.0; for minor revisions to a published document, increment the decimal number (ex. 1.1); for major content upgrades to a published document, increment the leading whole number (ex.2.0).

Version	Date	Author	Change Description
1.0	10/9/2024	Information Security and Privacy Office (ISPO)	Initial release

Publication Review and Approval History

A formal review of this document was conducted in accordance with City of Arlington requirements on the following dates:

Version	Date	Reviewer	Remark
1.0	11/18/2024	City Manager’s Office	Approved

B. PURPOSE

This policy is intended to outline the security measures and guidelines for the responsible use of generative AI technologies within the City. It ensures that AI models, data inputs, and outputs are managed in a manner that protects sensitive information and prevents misuse or unintended consequences.

C. SCOPE

All City officials, employees, departments, vendors, contractors, and volunteers who operate on behalf of the City are subject to this policy.

D. EFFECTIVE DATE & IMPLEMENTATION

This citywide policy becomes effective on the date it is approved.

E. POLICY

Roles and Responsibilities

- **Department Directors** –Department Directors at the City hold the ultimate responsibility for ensuring “all users” associated with their department comply with the requirement within this policy.

Policy Requirements

1. **Use of Generative AI Outputs**

   a. The outputs of Generative AI systems must be reviewed by the City employee who generated them or their supervisor before being used in any official City capacity.

2. **Data Security and Privacy**

   a. Use of AI systems shall be consistent with all other City security, technology, data governance, and record management policies, procedures, and standards.

   b. **Public or Uncontrolled Generative AI**

   Confidential data should not be entered into public AI systems or models. Public or uncontrolled AI refers to those not controlled by the City, have access to City inputs, or utilize City data to train an AI model made available to the public or other customers.

   Examples include, but are not limited to ChatGPT, Google Bard, Microsoft Copilot, Copy.ai, Grammarly, Firefiles.ai, Scribe, and Otter.ai. When in doubt, reach out to the Information Security and Privacy Office.

   c. City-controlled or private Generative AI

   Unless the operating effectiveness of security and privacy controls have been verified by the Information Security and Privacy Office's review, employees shall not submit data classified as Confidential, or that are otherwise not considered to be acceptable to disclose to the public, to any City-controlled or private AI system. City-controlled or private AI refers to systems controlled by and only accessible to the City.

3. **Security and Privacy Incident Reporting**
    a. Any breach, unauthorized access, or misuse of an AI system, including entry of Confidential data into Public or Uncontrolled AI systems, must be reported to the Information Security and Privacy Office, per the Security Incident Response Plan.

4. **Public Records & City Records Management**
    a. All records generated, used, or stored by Generative AI systems may be considered public records and must be disclosed upon request.

    b. City employees who use Generative AI systems are required to maintain, or be able to retrieve upon request, records of inputs, prompts, and outputs in a manner consistent with the Texas Public Information Act and City record management policies.

F. EXCEPTIONS

Any exceptions to Policies can introduce significant risk, which requires written acceptance by the relevant Department Director acknowledging and accepting the risk, and then review and acceptance by the Information Security and Privacy Office.

G. NON-COMPLIANCE

For City staff, non-compliance with citywide policies and standards is subject to disciplinary action in accordance with the Human Resources Disciplinary Policy. For vendors, non-compliance may result in suspension of access, termination of contract(s), legal action, and loss of future business with the City.

H. APPROVAL AUTHORITY

- All information security and privacy **policies** that apply on a **citywide** basis shall be approved by the City Manager's Office.

- All information security and privacy **standards and procedures** that apply on a **citywide** basis shall be approved by Chief Information Security Officer or their delegate. The Chief Information Security Officer, or their delegate, is responsible for notifying the IT Steering Committee for any changes related to technology.

- **Departmental** policies, standards, and procedures can be approved through each respective department's internal workflow. Citywide information security and privacy policies take precedence, but departments may develop policies, procedures, or standards that are more restrictive than the City's citywide policies, procedures, or standards if deemed necessary. It's recommended that the department consult with the Information Security and Privacy Office for review.

I. MAINTENANCE

This policy will be maintained through the Information Security and Privacy Office. Maintenance includes but is not limited to: (1) interpretation and monitoring annual compliance by City Departments; (2) ensuring this policy content is kept current; and (3) assisting City Departments with understanding how to comply with this policy.

J. DEFINITIONS

All definitions are contained within the City's Information Security Policy Glossary.

K. RELEVANT STATUTES AND LEGAL OBILIGATIONS

- FBI Criminal Justice Information Services (CJIS) Security Policy
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, and all regulations adopted to implement HIPAA
- Texas Business and Commerce Code Section 521.053
- Texas Government Code Section 254.133; 2054.135; 2054.136; 2054.603
- Texas Government Code Section 620.003
- Texas Government Code Section 559.003
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
- PCI Data Security Standard (PCI DSS)
- America's Water Infrastructure Act (AWIA) Section 2013/SDWA Section 1433
- NIST 800-53 Rev. 5
- NIST Cybersecurity Framework (CSF) 2.0