ARLINGTON℠

THE AMERICAN DREAM CITY

Data Classification 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 define a framework for categorizing the City's data criticality levels based on its level of risk. The City's three classification levels are Public, Controlled, and Confidential, which ensures that appropriate security measures are applied to protect the City most sensitive data throughout its lifecycle, support adherence to compliance and legal obligations, and mitigate the risks of unauthorized access, disclosure, or loss.

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 REQUIREMENTS

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

All City data and information should be classified in one of the classes below. Most City data will fall into Public and Confidential

Class	Description	Examples (non-exhaustive list)
Public	City data not otherwise identified as Confidential or Controlled data, and: 1. Publicly available 2. No requirement for confidentiality, integrity, availability, or safety	• Information authorized to be available on or through CoA website (without login) • Most City maps • Job postings
Controlled	City data not otherwise identified as Public or Confidential, and: 1. Not publicly available 2. Publicly releasable in accordance with the Texas Public Information Act	• Employee names • Employee salary information • Most policies and manuals • Most internal emails and chat messages

Class	Description	Examples (non-exhaustive list)
Confidential	Data exempt from public disclosure requirements under the provisions of applicable state or federal law.	• Social Security numbers • Access device numbers (building access code, etc.) • Biometric identifiers (eye images, full face images, fingerprints, etc.) • Date of birth • Driver's license numbers • Passport and visa numbers • Personal vehicle information • Financial information and records (credit card numbers, account numbers, etc.) • Certain management information • Passwords • User ID Numbers • Health Information, including Protected Health Information (PHI) • Health Insurance policy ID numbers • Most information related to information, cyber, or physical security • Criminal Justice Information • Critical infrastructure information (i.e., AWU plant diagrams, traffic system diagrams)

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