	Responsible Department:	**Effective Date:** 12/21/2021
	Approvals: Jim Thompson, City Manager Bianca Lochner, Chief Information Officer	**Date Approved:** 12/21/2021

1.0 PURPOSE

1.1. The purpose of this Administrative Regulation (AR) is to safeguard the public's trust in the City's use of new and emerging technologies and to protect their digital privacy rights. It sets forth the framework for City departments to observe when information systems or other applications and forms collect the public's Personally Identifiable Information (PII). This AR strives, to the extent practicable, to enable residents to determine for themselves when, how, and to what extent information about them is communicated to others.

As new and emerging technologies have a greater capacity for collecting information and drawing insights about people and communities, a Digital Privacy AR will enable the City to harness the power of those insights to provide better services to the community while ensuring that personal and sensitive information is properly protected.

2.0 APPLICABILITY

2.1. This AR applies to all employees who are responsible for the procurement, implementation, support and use of technology that collects, analyzes, stores, and retains digital information.

3.0 POLICY

3.1. It is the policy of the City to protect the privacy of individuals and the digital form of any Personally Identifiable Information that is collected, used, shared, stored or retained by the City. In addition to this Policy, the City is also subject to laws and regulations that govern the information collected.

3.2. To the extent permissible by law, City departments will adhere to the following Privacy Principles:

3.2.1. **Notice:** Providing notice about the collection, use, and sharing of personal information at the time such information is collected. The City will make every reasonable effort to provide a privacy notice when basic municipal services are requested or delivered.

3.2.2. **Retention:** Developing, maintaining, and following the City's data retention schedule. Departments must ensure that identifying information is deleted or deidentified after the retention period expires. In the event of a conflict between this AR and the Public Records Act (A.R.S. § 39-101 et seq.) or other law governing the disclosure of records, other applicable

law will determine our obligation in support of open and transparent government. See Arizona's Public Record Law.

3.2.3. **Minimization:** Minimizing the collection and processing of identifying information and limiting collection to only what is necessary to provide services and to conduct business. When personally identifiable data is required to deliver or improve service, departments, and city contractors, must anonymize, de-identify, pseudonymize, or otherwise mask this information unless certain personally identifiable data is necessary to provide the service, or the service is provided through a contract which specifically addresses this issue.

3.2.4. **Accountability:** Maintaining documentation, available for public review and third-party monitoring, to evidence compliance with this AR. If any information under the City's control is compromised or if residents are impacted due to a breach of security or negligent maintenance of information systems, the City will take reasonable steps to investigate the situation and notify those individuals whose information may have been impacted.

3.2.5. **Accuracy:** Making every reasonable effort to provide the public with information on how predictive or automated systems are used and instituting processes to correct inaccurate information or methodologies in those systems.

3.2.6. **Sharing:** Following clear data governance procedures and instituting information-sharing agreements when sharing information with outside entities, which shall strive to enable effective information sharing while following this AR.

3.2.7. **Equity:** Being mindful of the populations the City serves and how data about members of the public, including vulnerable populations, can and should be used.

4.0 PROCEDURES

4.1. The City Manager or designee will lead the citywide implementation, maintenance, and adherence to this AR in coordination with the Digital Privacy Steering Committee, City Departments and Departmental Privacy Representatives. The City Manager or designee, in partnership with the Digital Privacy Steering Committee and City departments, shall approve technologies and projects according to this AR.

Implementation of the AR shall include at least the following:

4.1.1. Establishing a Digital Privacy Steering Committee comprised of senior management responsible for developing and implementing processes and procedures required for implementation and ongoing oversight of this AR.

4.1.2. Developing procedures for prioritizing and executing the evaluation of privacy risks for new projects and vendor contracts according to this AR and the interests expressed by the City Council and community members; and

4.1.3. Privacy review and assessment processes to aid departments and information system owners in ensuring that digital privacy standards in this

AR are integrated into technologies, projects, processes, and vendor contracts.

At the recommendation of the Departmental Privacy Representatives and in accordance with the standards in this AR, the City Manager or designee may require departments to make modifications to technologies or projects to comply with this policy.

4.2. The City Manager or designee will work with the city's departments to:

4.2.1. Identify Departmental Privacy Representatives responsible for overseeing projects and initiatives to ensure compliance with this AR.

4.2.2. Develop and implement a process for determining the relative level of risk and public benefit associated with the use of Personally Identifiable Information that is collected, used, shared, stored, or retained by the City.

4.2.3. Develop and implement a process to solicit citizen input and feedback regarding the use of Personally Identifiable Information that is collected, used, shared, stored, or retained by the City.

4.2.4. Develop and implement processes and procedures for safeguarding Personally Identifiable Information that is collected, used, shared, stored, or retained by the City.

4.3. Exceptions

4.3.1. Due to the individualized and serious nature of emergency response efforts, a variety of personally identifying information may be collected by first responders and other personnel, as needed, and such data collection, use and disclosure practices will be covered under Public Safety policies.

4.3.2. This Policy does not apply to personal/personnel information obtained in the city's capacity as an employer. Employment information is covered under separate Human Resources policies.

4.3.3. This Policy specifically does not preempt policies already in existence at the departmental level, including local, state, and federal laws, or other regulations that govern the operations of departments within the City.

5.0 RESPONSIBILITIES

5.1. All city employees shall follow the policies and procedures outlined in this AR.

5.2. Upper level management is responsible to ensure the overall management of this AR, including the appointment of Departmental Privacy Representatives, within their respective divisions, departments, or offices.

5.3. The City Manager or designee is responsible for coordinating the overall implementation, communication, and training regarding this AR.

5.4. The Departmental Privacy Representatives are responsible for their department's implementation of and compliance with this AR.

5.5. The Communications and Public Affairs Director or designee is responsible for developing and leading the public engagement and outreach process under this AR.

6.0 OVERSIGHT/REVIEW

6.1. Departmental Privacy Representatives shall receive training concerning this AR and specific division, department or office policies and procedures, appropriate to their assigned duties.

6.2. This AR will be reviewed as needed, but no less frequently than every three years.

7.0 DEFINITIONS

7.1. **Personally Identifiable Information (PII):** Information in the possession of the City that can directly or indirectly identify individuals. This information can be classified into four primary categories of data:

7.1.1. Personal data: information relating to an individual, such as full name, street address, email address, and personal computer or mobile device IP address.

7.1.2. Image data: digital pictures or photographs that can identify an individual by their face or other contextual information.

7.1.3. Recording data: audio or video information that can identify an individual by their face, voice, or other contextual information.

7.1.4. Geolocation data: information affiliated with a computer, device, or vehicle that can be used to identify an individual based on physical location or on aggregate location patterns.

7.2. **Tracking Technology:** Any technology that collects, stores, or transmits Personally Identifiable Information that can be used to identify, monitor, surveil, make inferences about, or predict the behavior of individuals.

8.0 RELATIONSHIPS TO ADOPTED POLICIES AND ORDINANCES

8.1. Federal/State Law

8.1.1. State of Arizona Public Records Guidelines

8.1.2. Data Security Breach

8.2. Arizona Public Records Law

8.3. City Charter/Ordinance

8.4. Other Administrative Regulations

8.4.1. AR295 Citywide Records Management Program

8.4.2. AR296 Records Requests

8.4.3. AR297 Open Data Program

9.0 LINKS TO SUPPORTING DOCUMENTS

10.0 REVIEWED/AMENDED DATE(S) AND NOTES ON SIGNIFICANT CHANGES:

10.1. Original Effective Date.

10.2. Each time the AR is reviewed, the review date should be added. For all substantive updates, a brief explanation of the sections changed and the rationale for changes should be added as a guide to the reader.