Chapter 3.39 City Data and Privacy Office

3.39.010 Organization.

The City Data and Privacy Office will be an independent office managed by the Chief Data Officer (CDO) who reports to the City Administrator.

3.39.020 Duties and Responsibilities.

The City Data and Privacy Office is responsible for the following:

A. Data governance.

1. Establishing a city-wide data governance framework to ensure data usability and integrity, acting as the single point of contact for City data governance and ensuring adherence across City offices.

2. Adopting policies, and technical standards consistent with this Chapter, including regarding the collection, use, management, retention, and sharing of City data and metadata.

3. Acting as the lead entity responsible for advising the City Administrator on administrative rules and rule changes consistent with this Chapter.

4. Collaborating with the Bureau of Technology Services to promote the development and support of enterprise data management and software solutions to ensure data governance needs guide information technology decisions, and that information technology planning supports long-term stewardship of City data assets.

5. Providing bureaus with best practices, training, and technical guidance to conform to data governance standards established pursuant to this Chapter, with an emphasis on secure handling of sensitive data and compliance with data minimization principles.

6. Advising the City, in concert with the City Attorney and other appropriate bodies, on policies, practices, and decisions related to which City data sets may be appropriate for public disclosure, balancing City interest in transparency with its obligation to protect citizen privacy and security.

7. Advising the City, in concert with the City Attorney and other appropriate bodies, on policies, practices, and decisions that implicate the interests of this Chapter in City public records and information released in public records requests,

specifically balancing City interest in transparency with its obligation to protect citizen privacy and security.

8. Advising the City on the development of contracts, including but not limited to intergovernmental agreements, procurement contracts, and grant agreements that implicate sensitive data, providing, as appropriate, modifications, conditions, or prohibitions to ensure consistency with City data governance and privacy standards.

9. Conducting audits and assessments of City data management policies and practices to ensure compliance with established policies and best practice, including Sanctuary protections and open data principles.

B. Surveillance and privacy oversight.

1. Conducting reviews of City programs and pilots that implicate sensitive data, surveillance technologies, artificial intelligence systems, large language models, and other automated decision systems. This shall include Privacy Impact Assessments (PIAs) completed prior to the deployment of a program or pilot when that program or pilot is new, or for existing programs or pilots, when they incorporate a change that implicates sensitive data such as a different scope of work, technological capabilities, a new vendor, or similar.

2. Maintaining the City-wide Surveillance Technology Inventory.

3. Adopting policies and collaborating with the Bureau of Technology Services on technical standards consistent with this Chapter, including regarding the acquisition, use, management, retention, and sharing of technologies implicated in this Chapter, including the information collected by or derived from the technologies.

4. Acting as the lead entity responsible for advising the City Administrator on administrative rules and rule changes consistent with this Chapter including those related to surveillance and privacy oversight.

5. Advising Council on the development of City Code consistent with this Chapter, including for Title 34 Digital Justice.

6. Advising the City on planning, policy development, public engagement, and budgeting efforts that implicate surveillance technology and privacy.

7. Conducting, in concert with relevant City entities, community engagement to inform the development of and gather feedback on City surveillance technologies and privacy practices.

8. Conducting audits of bureau and vendor surveillance and privacy practices, advising the City Administrator and City entity managing the contract on corrective action for noncompliance as appropriate.

C. Reporting.

1. Submitting an annual report to the City Council regarding:

a. The City's acquisition and use of technologies implicated in this Chapter;

b. City Bureau and vendor compliance with City privacy and data governance standards; and

c. Recommended data governance, surveillance technology, automated decision-making technology, and privacy policies to be developed or amended to advance City values and address City and community needs.