City of Sugar Land Data Sharing Process and Guidelines

Creation Date: June 2025

1. Purpose

The City of Sugar Land manages a substantial amount of data, considered a key asset, which includes personally identifiable information (PII) regarding both residents and employees. While promoting data-driven insights is a priority, the City is committed to sharing data responsibly, ensuring that sensitive data is protected and shared in compliance with state and federal laws.

This document aims to establish internal processes for evaluating and responding to data access requests, particularly those involving non-public information, while upholding the City's obligations under the Texas Public Information Act (TPIA), the primary law governing access to government records.

2. Scope

These guidelines apply to:

- Internal city employees requesting access to sensitive or restricted data from other departments.
- External requests for non-public data that are not already available through the City's Open Data Portal.

Exclusions: These guidelines do not apply to:

1. Requests that have already been formally submitted under the TPIA.
2. Data involved in ongoing litigation or subject to legal holds.
3. Data that is publicly available on the Sugar Land Open Data Portal.
4. Data shared under existing city contracts with vendors or agencies.

Note on Public Records Requests:

All external data requests are subject to evaluation under the TPIA (Texas Government Code Chapter 552). Requests for information that qualify as public information under the TPIA must be processed according to the Act's requirements, including required disclosures, redactions, review of exceptions, and response deadlines. These guidelines do not override the TPIA and are intended only for handling non-TPIA data requests (e.g. collaborative research, interagency data exchange).

3. Roles and Responsibilities

Data Owner: The department with subject-matter expertise and operational authority over a given data set. Responsible for data accuracy and quality.
Data Steward: A designated employee or group responsible for gathering the relevant datasets and metadata from the Data Owner and preparing them for sharing, consistent with City policy.
Data Requester: Any internal or external entity seeking access to non-public data.
Data Governance Committee: Group responsible for overseeing the implementation of data policies and agreements.
Legal Department: Responsible for determining the legality and risk of data sharing and preparing Data Sharing Agreements.
Office of Data and Innovation: Central point of contact for coordinating data access and governance.
Data Program Manager: Reviews documents and prepares datasets related to data requests.
City Clerk's Office: Responsible for reviewing and responding to TPIA requests.

4. Data Sharing Process

4.1 Internal Data Sharing

Internal requesters seeking access to sensitive or restricted data must fill out a data request form clearly stating the purpose of the request and submit the completed form to IT. If IT does not have access to the required dataset, the internal requester will be guided to contact the respective Data Owner. The leadership team of Data Owner will decide on whether to grant access. If access is granted, necessary accounts or access credentials will be created or assigned.

4.2 External Data Sharing

4.2.1 All external requests for data must first be screened for applicability under the TPIA. If a request is determined to fall under the TPIA, the City Clerk's Office will process the request under standard procedures. If a request falls outside the scope of the TPIA (e.g. voluntary data-sharing for academic collaboration or intergovernmental agreement), the process below may apply.

4.2.2 Where external entities (such as state agencies, academic institutions, or private organizations) request non-public data for valid research, planning, or partnership purposes outside of the TPIA, the following process applies:

1. *Initiate Request*: The Data Requester submits a written request to the Office of Data and Innovation. The request must include the purpose,

specific data elements sought, intended use, and anticipated duration of the data access.

2. *Initial Review and Eligibility Assessment: The* Office of Data reviews the request to determine whether it meets a legitimate business, research, or public interest purpose and whether it aligns with City policies and priorities. If the request is ineligible, the process ends here with a written explanation to the Data Requester.
3. *Data Owner Consultation and Risk Review:* For eligible requests, the Office of Data and Innovation consults the relevant Data Owner(s) to confirm data availability and assess whether the data can be shared. As part of this review, the Office of Data and Innovation will coordinate with the Legal Department as needed to evaluate privacy concerns, legal restrictions, or risks of disclosure, particularly where PII or sensitive data is involved.
4. *Legal Agreement and Data Preparation*: If the request is approved, the Legal Department drafts a Data Sharing Agreement (DSA) detailing the scope of data use, security requirements, and data protection measures. The Data Steward coordinates with the Office of Data and Innovation to compile and format the dataset.
5. *Approval*: The Data Program Manager conducts a final review of the DSA and prepares the dataset to ensure data is relevant to the approved request, appropriately limited in scope, and adequately protected, particularly with respect to PII or other sensitive data.
6. *Execution and Transfer*: The DSA is sent to the external requester for signature before data transfer is authorized. Once the DSA is signed, the dataset is securely transferred using encrypted or protected methods (e.g. encrypted emails, SSL/TLS-encrypted file sharing services, or secure FTP (SFTP)) to safeguard the data against unauthorized access.
7. *Post-Transfer Oversight*: The Office of Data and Innovation may monitor compliance with the terms of the DSA. In the event of any misuse, unauthorized disclosure, or breach of agreement, access may be terminated and appropriate legal or contractual remedies may be pursued.

5. Training and Awareness

The Office of Data and Innovation will conduct annual training on how the TPIA applies to data requests, internal processes for reviewing and handling sensitive or restricted datasets, and data security protocols for handling PII.

6. Contact Information

dataandinnovation@sugarlandtx.gov