DATA GOVERNANCE POLICY

Policy Number:
Creation Date: September 2023
Revised Date:
Sunset Date: September 2027

OVERVIEW & PURPOSE

The City of Sugar Land generates, stores, and utilizes vast amounts of data in every operational area. The City considers data an asset and has committed to governing it as such in the Data Governance Charter. This document supplements the Charter and sets forth policies and standards to support:

- Data privacy and security by safeguarding the City's data assets and respecting residents' right to privacy.
- Data management by establishing comprehensive data inventory practices for the City of Sugar Land.
- The City's commitment to transparency through open, accessible, and high-quality data by establishing best practices for Open Data Portal creation and maintenance.

APPLICABILITY

This policy applies to all Departments and Offices of the City of Sugar Land.

DEFINITIONS

- **Critical Infrastructure -** Public or private assets, systems, and functions vital to the security, governance, public health and safety, economy, or morale of the state or the nation.[i]
- **Critical Infrastructure Information -** Information not customarily in the public domain and related to the security of critical infrastructure or protected systems.
- **Dataset** – A collection of related data presented in tabular or non-tabular form that can be pulled from a data source.
- **Data Governance** - A set of policies, processes, and tools that ensure data quality, accessibility, usability, integrity, and the overall readiness of data that is used to make business decisions intended to create, improve, or sustain services and products.
- **Data Inventory** – A fully described record of the data assets maintained by an organization.
- **Data Source** – A system, database, or other information source that contains and reports raw data.
- **Data Steward** - Designated individual(s) from each department who serve as primary points of contact and accountability for their respective departments as related to data projects and needs. These individuals should have business knowledge of the data and can answer questions about the databases, datasets, or information systems used within the department.
- **Metadata** - Any information that is used to provide descriptive detail about a dataset, including but not limited to, the date range, a description, or the owner.
- **Open Data** - Data that is made available to the public consistent with any and all applicable laws, rules, regulations, ordinances, resolutions, policies or other legal restrictions, requirements or

rights associated with the data. Data will not be Open Data if it meets the definition of Private, Protected, or Sensitive Information.

- **Open Data Portal** - A single web portal owned and maintained by the City that will be the repository and public access point for Open Data.
- **Open Format** - Any widely accepted, nonproprietary, platform-independent, machine-readable data format, which permits automated processing of such data and facilitates analysis and search capabilities.
- **Personally Identifiable Information (PII)** - Any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources. It includes information that is linked or linkable to an individual, such as medical, educational, financial and employment information such as the following is Private Information.
    - PII alone-
        - Social Security number (There are additional restrictions on where Social Security numbers can be stored and shared.)
        - National ID number, passport number or Visa permit number
        - Driver's license number
        - Bank and credit/debit card numbers
        - Tax information (e.g., W-2, W-4, 1099)
        - Telephone number
        - Email address
    - PII when combined with other information-
        - Disability information
        - Race and/or ethnicity
        - Gender
        - The location of an individual at a particular time
        - Web sites visited
        - Materials downloaded
        - Any other information reflecting preferences and behaviors of an individual
- **Protected Information** - Any dataset, or portion thereof, to which the City may deny access pursuant to The Texas Public Information Act (Texas Government Code Chapter 552) any other applicable law, rule, regulation, court order or as otherwise required. Protected information includes data that the City is prohibited from disclosing by operation of law or that is subject to strict handling requirements dictated by statutes, regulations, or legal agreements including but not limited to:
    - Health Insurance Portability and Accountability Act (HIPAA),
    - Driver's Privacy Protection Act,
    - Fair Credit Reporting Act,
    - Family Education Rights and Privacy Act (FERPA)
    - Critical Infrastructure Information (PPD-21 and Texas Govt Code 418.181)
    - Criminal Justice System Information (CJIS)
    - Texas Public Information Act (TPIA)
    - Texas Medical Privacy Act (TMPA)
    - Payment Card Industry Security Standards (PCI)

- **Sensitive Information** - Any data which, if published by the City online, could raise privacy, confidentiality, proprietary or security concerns or have the potential to jeopardize public health, safety or welfare to an extent that is greater than the potential public benefit of publishing that data.

POLICY SECTIONS

DATA PRIVACY

The City will protect the rights of all individuals and the digital form of any Private, Secure, and Protected Information that is collected, used, shared, and/or stored by the City. In addition to this policy, the City is also subject to laws and regulations that govern the information collected. The guidance set forth in this section is relevant to:

- All data processed, stored, and/or transmitted by a City of Sugar Land Information Technology System(s).
- All City of Sugar Land data processed, stored, and/or transmitted on personally owned devices also referred to as Bring Your Own Device (BYOD).
- All data collected or maintained on a City of Sugar Land owned and managed network or authorized/contracted cloud platform by, or on behalf of, COSL in any form including electronic or hardcopy.
- All employees, departments, and third-party service providers who handle data on behalf of the City of Sugar Land.

I. **Purpose of Data Collection**

The City collects and processes Personally Identifiable Information for purposes including but not limited to:

- Providing and improving City services, programs, and activities
- Processing payments, permits, licenses, and other transactions
- Responding to inquiries and requests
- Enhancing public safety
- Conducting research and analysis
- Complying with legal and regulatory obligations

II. **Types of Information Collected**

Within the scope of providing essential City services, The City of Sugar Land may collect and process various types of information, including but not limited to:

- Personally Identifiable Information
- Demographic Information: Age, gender, ethnicity, and other relevant demographic data
- Financial Information: Payment details, tax information, other financial records for processing transactions
- Communication Information: Records of communication with the city, including e-mails, correspondence, and feedback.

- Location Information: Geographical data for service delivery, such as emergency services, mapping, and utilities.
- Website Usage Information: IP Addresses, cookies and browsing behavior from City sanctioned websites.

III. **Data Sharing and Disclosure**

This section outlines how, and when, the City may share or disclose information in certain circumstances.

- **Sharing within the City of Sugar Land:** The City of Sugar Land may share Personally Identifiable Information, Protected Information, and Sensitive Information within various departments and divisions to provide residents with efficient and effective services. Access to this information is restricted to authorized personnel who have a legitimate need to access it for official purposes.
- **Third Party Service Providers, Contractors, and Partners:** In some cases, the City may engage third-party service providers and contractors to assist in service delivery. These providers may have access to Protected Information or Sensitive Information only to the extent necessary for them to perform their services. The City of Sugar Land will take reasonable steps to ensure that these service providers adhere to strict confidentiality and security measures to safeguard private information. These steps include the use of a standardized Data Sharing Agreement (DSA). Departments engaging with partners or vendors via Memorandums of Understanding or contracts should consult with Legal to ensure that data exchanges are fully and accurately documented in a DSA. The standard DSA shall establish the purpose of the exchange, terms of use, nondisclosure of confidential information, and requirements for storing and destroying data.
- **Public Requests and Open Records:** Certain information held by the City of Sugar Land may be subject to public records requests under applicable laws. This means that private information could be disclosed to individuals or entities requesting access to public records unless such disclosure is prohibited by law.

IV. **Procedures and responsibilities**

City departments will adhere to this policy based on including the following elements to protect individual privacy:

- **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 Information is required to deliver or improve a service, departments must redact this information when sharing it with individuals who do not need access to the Personally Identifiable Information.
- **Accountability:** Maintaining documentation, available for public review and third-party monitoring, to evidence compliance with our privacy principles and policy. If any information under our 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. If a third-party provider realizes that information

from the City has been breached, they must notify the impacted individuals and the City within a timely manner.

- **Accuracy:** Making every reasonable effort to provide the public with information on how predictive or automated systems are used and will institute processes to correct inaccurate information or methodologies in those systems. City Departments may use predictive or automated systems and technologies to support decision making, but some degree of human input and oversight into decision making is also required.

DATA INVENTORY

Managing data as an asset requires a complete understanding of the range, type, and location of data in the City. A data inventory sets the foundation for:

- *Increased awareness* of data assets by providing a clear picture of the data owned, collected, and maintained throughout the organization.
- *Enhanced information security* by identifying private, protected, or sensitive information in datasets and ensuring that proper actions are being taken to safeguard it. This process will allow for the organization to identify and address any gaps in protection.
- *Prioritization of data* for public access through an open data portal.
- *Enhanced efficiency* for internal collaboration by limiting the number of steps and time it takes to access another department's data.

I. Each department must create and maintain a data inventory to include data sources and datasets. Departments should make reasonable effort to catalog as many data sources and datasets as possible, including the associated metadata. Department inventories must be regularly maintained and updated on an annual basis according to the guidelines set in place by the Director of Data and Innovation.

II. Data Stewards are assigned to each department and are responsible for coordinating the inventory process in a way that works best for their respective departments. Guidance for completing department data inventories will be provided during the annual update period.

III. The Director of Data and Innovation oversees the initial inventory process across the organization and ensures that annual updates are completed by each department. The Director of Data and Innovation and their team consolidates the individual department inventories into a single organization-wide inventory and ensures it is published and accessible to the entire organization.

OPEN DATA

The City creates, maintains, and stores a vast amount of data. The City is committed to identifying which of these data can be shared openly. While the City's data is necessary for normal operations, it also has the potential to produce a myriad of additional benefits as open data, such as:

- *Increase transparency* by allowing external parties to freely view data and create an enhanced understanding of City operations and priorities.
- *Empower citizens, businesses, and potential partners* to identify opportunity for innovation and partnership by allowing them to access, reuse, and analyze available data.
- *Proactively provide* information currently sought out through public records requests under the Texas Public Information Act.[ii]

- *Foster Departmental Collaboration* by making information easily shareable across the organization.
- *Enhance Decision Making* through readily available data and analytics tools.

The guidance set forth in this section is relevant to all data chosen, or being considered, for open and public release.

I. **Portal**
   i. The City of Sugar Land's Open Data Portal will serve as a centralized location for Open Data produced and collected by City Departments and employees. The Portal will be hosted on the City's public website or another suitable online location.
   ii. Data published on the Open Data Portal should be accessible, downloadable, and in an open format.
   iii. The Portal will provide a method for the public to offer input on the open data program, share what data they feel should be prioritized for publication, and give feedback on the quality and usefulness of published data.
   iv. The portal's technical functionality will be maintained by the Department of Data and Innovation and the Department of Information Technology in conjunction with the chosen vendor's technical team.
   v. The Department of Data and Innovation and Department of Information Technology will collaborate to ensure that the Portal and its features are up to date with ever-changing technological advancements.
   vi. The Department of Data and Innovation will be responsible for managing the vendor relationships, entering and renewing associated contract(s), and funding the open data program.
   vii. The Department of Data and Innovation will provide annual reports to the organization on portal traffic, pain points, and opportunities for improvement.

II. **Publication Procedures**
   i. The Data Governance Committee will be responsible for determining publication standards and priorities. The Committee will account for public and organizational demand, privacy and sensitivity guidelines, and readiness when creating the metric or rubric used for prioritization.
   ii. The Department of Data and Innovation will provide Departments with resources and guidance on how to determine which of their datasets are good fits for publication.
   iii. The Department of Data and Innovation will be responsible for creating the process and procedures for dataset submission.
   iv. The Department of Data and Innovation will review submissions and collaborate with Department Directors to ensure datasets are in a state fit for publication.
   v. The Data Governance Committee may be consulted in cases where the publishing Department or Data and Innovation would like more input on whether certain data is fit for publication. The Data Governance Committee also reserves the right to require departments publish certain datasets based on feedback, public demand, or executive request. Public demand may encompass but is not limited to open records requests, 311 inquiries, or direct resident requests via the portal.

vi. The Department of Data and Innovation and Information Technology representatives will work with the publishing Department on publication and maintenance procedures.

vii. Data deemed as Private, Protected, or Sensitive according to the standards listed in the Data Privacy section of this policy will not be considered for publication unless portions can be redacted to mitigate privacy or security risks. For instance, any datasets considered to be Critical Infrastructure, or that contain Protected Critical Infrastructure Information, according to state and/or federal law, will also be deemed ineligible for publication. Opportunities to aggregate, redact, and/or generalize related data to protect the integrity of such infrastructure will be considered.

viii. The Directors and Assistant Directors will have the ability to repeal datasets from publication with approval from the Data Governance Committee if they are able to present valid justification of privacy, security, or other risks presented with sharing said data.

ix. Full and complete metadata must be provided by the data steward for all data published on the portal.

III. **Disclaimers and Reservations**

i. Open Data available on the City's Open Data Portal will be published under the following disclaimer on the Portal website: "The City of Sugar Land does not warrant or make representations or endorsements as to any of the information listed on this website or any of the external links listed on this page. Data or datasets made available on the website are provided on an as-is basis and for informational purposes only. Such materials have been compiled from a variety of sources and are subject to change without notice from the City of Sugar Land. THE CITY OF SUGAR LAND MAKES NO REPRESENTATIONS OR WARRANTY AS TO THE COMPLETENESS, ACCURACY, QUALITY, TIMELINESS, CONTENT, OR ANY OTHER ASPECT OF ANY DATA MADE AVAILABLE THROUGH THIS SITE. THE CITY OF SUGAR LAND EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. The use of this data will be at the sole risk of the party using such data."

ii. The City reserves the right to discontinue availability of content on its Open Data Portal at any time and for any reason. Nothing in this policy will be construed to create a private right of action to enforce any provision of this policy. Failure to comply with any provision of this policy will not result in any liability to the City of Sugar Land.

RESPONSIBLE OFFICE

This policy shall be reviewed at least annually by the Data Governance Committee and the Department of Data and Innovation.

ENFORCEMENT

The Department of Data and Innovation is responsible for ensuring that all City Departments adhere to this policy. Nonconformance will result in notification of the appropriate Director or Executive Team member.

POLICY HISTORY

2023 – Policy created.

APPENDIX

- **Data Governance Charter**
- **Data Inventory Step-by-Step Guide**
- **City Website Policy**
- **Information Technology Security Policy**