Administrative Regulation No. 72

City of Cincinnati

Date: August 22, 2016
Revised: November 28, 2016

Office of the City Manager

Approved:

Subject: **Analytics Infrastructure Policy (Data Governance)**

1.0 INTRODUCTION

1.1 BACKGROUND

The City of Cincinnati seeks to deliver efficient, effective, and improved customer services at the lowest possible cost to our residents. One way the City can identify opportunities for improved delivery of services is through the effective use of data. A strong Analytics Infrastructure can help ensure that potential is maximized by providing a framework for the storage and use of data. Because there are a variety of departments which work together to deliver services to our customers, a key component of this Analytics Infrastructure is a clear Data Governance policy, which outlines the expectations for data access, availability, and management to ensure cross-functional decision-making, accountability, data integrity, and data availability.

1.2 OBJECTIVES

The specific objectives of our analytics infrastructure framework are to establish expectations and apply appropriate controls over:

- Data Inventory and Ownership
- Data Collection
- Data Use and Disclosure
- Data Availability, Retention and Disposal

1.3 INTENT

The City of Cincinnati is a steward of the data that is collected from residents and visitors and thus has a responsibility to protect that data. At the same time, the Office of the City Manager recognizes that the collected data is a valuable asset for managing the municipal enterprise and critical for identifying opportunities to improve the quality, effectiveness, and efficiency of service delivery to residents and customers of Cincinnati. The Office of the City Manager seeks to accomplish these goals of management and improvement through the Office of Performance and Data Analytics (OPDA). The City's and OPDA's capability to achieve these goals relies on a strong Analytics Infrastructure and direct access to municipal data in order to perform the following core functions related to this mission:

1. Automated data dashboarding to consistently monitor and evaluate performance.
2. Real-time monitoring of operations.
3. Self-Service Data Discovery - allowing departments to fluidly use data to gain insight about operations without relying on power users and database administrators for analysis.
4. Predictive Analytics - the ability to use data to develop predictive models that enable proactive and preventative service delivery to enhance operational effectiveness and efficiency. Open Data available to the public for transparency and to foster innovation.

Specifying standards, policies, procedures, and responsibilities with regard to data access, management and data related activities will help develop and maintain the infrastructure that promotes these functions.

While the Office of the City Manager expects departments to provide access and make data available to OPDA, it recognizes that some of the data collected and utilized by OPDA to fulfill its objectives is of a sensitive nature. To that end, the Office of the City Manager shall establish, implement, operate, monitor, review, maintain, and improve an Analytics Infrastructure framework that ensures requisite access to data by OPDA while also ensuring that appropriate controls are applied to data, and that the data is collected, used, and reported in line with compliance obligations.

1.4 SCOPE

Administrative Regulation XX applies to all departments and divisions of the City of Cincinnati. It applies to all forms of data including those in electronic and non-electronic form.

2.0 ANALYTICS INFRASTRUCTURE EXPECTATIONS

2.1 ***Analytics Infrastructure Policy.*** An Analytics Infrastructure Policy (Administrative Regulation 72) will be maintained, approved, published, and communicated to all city departments and divisions by the Office of the City Manager through the Office Performance and Data Analytics and Chief Data Officer. This policy will be reviewed and updated as required.

2.2 ***Analytics Infrastructure Procedures.*** The Analytics Infrastructure Policy (Administrative Regulation 72) includes the processes and procedures to be followed in order to fulfill its policy objectives. The Analytics Infrastructure Procedure will be reviewed quarterly as part of the regular meetings between the Chief Data Officer (CDO), Business Owners, and Source System Data Managers (SSDMs). It will be updated as required and summaries of any updates will be sent to all departments.

2.3 ***Open Availability of Data.*** The City is a steward of the data that it collects from residents and visitors. No one person, department, division, or group has exclusive access to City of Cincinnati data. While departments are responsible for the management of data they have collected, any other department can request access to any data. These requests may be subject to legal limitations to project personally identifying information (PII), such as HIPAA or CJIS, as well as any internal security procedures the City of Cincinnati has developed to protect data. If a request for data is denied, the reasons for the denial shall be provided to the requesting agency, which will have an opportunity to modify its request.

2.4 ***Data Collection.*** Data will be collected in a lawful and appropriate manner in accordance with the requirements of applicable legislation and any additional processes agreed upon by the departments requesting and providing the data in order to protect PII or sensitive data (Section 4.3.9).

2.5 ***Automatic Extraction of Data.*** If data is shared between departments, for example to improve the delivery of a service or so OPDA can monitor the performance of a department, that data shall automatically be extracted, transferred, and loaded to a secure, external computer warehouse. The location of the data must be approved by OPDA, even if OPDA is not the requesting department, to ensure there are no unnecessary restrictions preventing access to the data. Automatic extraction and collection will allow departments to efficiently and immediately use data. If a department has concerns regarding security or personally identifying information (PII), it will document those concerns and develop a separate agreement with the requesting department outlining why the information is not being automatically extracted, the schedule for extraction, and the safeguards established for data of concern. This separate agreement will be attached to the Letter of Intent initially sent by the requesting department (Section 4.3.7). All efforts will be made to ensure that data is not pulled during high volume times to minimize disruptions of departmental operations. Evaluations of current data sharing processes will be evaluated at the regular meetings between the Chief Data Officer, the Business Owners, and the Source System Data Managers.

2.6 ***Data Use & Disclosure.*** Data will be used and disclosed in a lawful and appropriate manner in accordance with the requirements of applicable legislation and any signed City of Cincinnati data use agreement. Unless it is specifically requested through a public records request (Section 2.8), data will not be redistributed in its raw form without the specific written permission of the originally collecting department. But aggregated data that does not contain personally identifiable information (PII) may be shared as part of reports to the city and outreach to the general public. When aggregating data, departments specifically review outliers to minimize the extent to which those outliers allow for personal identification.

2.7 ***Data Retention and Disposal.*** Data will be retained and disposed of in a lawful and appropriate manner in accordance to the City of Cincinnati's Security and Record Retention policies. If a department has extracted data from another department, it is responsible for disposing of that data at the end of the appropriate retention period or, if it chooses to retain the data for a longer period of time, informing the original collecting department of its choice and appropriately publicizing that information in compliance with Ohio law.

2.8 ***Responses to Records Requests.*** Each department is responsible for responding to records requests. For the purposes of Ohio public records laws, the originally collecting department shall be considered the department that "owns" the data. If OPDA or other department receives a request for records that it has extracted from another department, it will inform the original collecting department of that request and that department shall be responsible for responding to the request. OPDA or other extracting departments shall be responsible for responding to a records request only if the requested records were retained by the extracting department and not by the originally collecting department beyond the relevant retention period.

2.9 ***Third Party IT Solutions & IT Procurement.*** A department which believes it does not have the technology necessary to achieve one of its goals must approach IT Governance to determine whether there is an in-house solution before contacting any outside vendors.

If an in-house solution is not available, the Purchasing Division, in conjunction with the Enterprise Technology Solutions department and the IT Governance team, must work with the department and the third-party vendor to ensure there is specific language included in the contract to ensure data will remain properly open to the City of Cincinnati for access and analysis. IT Governance, the Chief Data Officer, and the Department should also consider:

Accessibility

- Whether the number of individuals/accounts who have access is limited.
- Whether the contract involves use of products from other external vendors who may limit access.

Control

- Who has ownership of the data.
- Whether the third-party provider may change the agreement terms at any time at the provider's discretion.
- The scope of any license to use intellectual property.

Services

- The services and assistance provided.
- How fast the provider will respond to a service or assistance request.
- The functionalities provided and how they relate to the department's desired goals and outcomes.
- Whether the purchased product or service interfaces with current technology data systems utilized in Cincinnati.
- Whether features are current and how long those features will be supported.
- How frequently and at what times servers may be maintenanced.

Security

- Whether the security used by the provider conforms to the security standards set by the City of Cincinnati.

The above should not be considered an exhaustive list of questions or factors for consideration as part of this process. The intent of these questions is to spur the Department to comprehensively consider its goals in entering a contract, and how it can best align with the City's goals and priorities. From the standpoint of this Administrative Regulation and data governance, the specific expectation with any IT procurement is that the Chief Data Officer and the Department work to clearly identify data access expectations with the vendor, and codify those expectations into the contract.

3.0 ANALYTICS INFRASTRUCTURE ROLES & RESPONSIBILITIES

The roles and responsibilities outlined below will govern management, access, and accountability for the City of Cincinnati Analytics Infrastructure.

3.1 Chief Performance Officer (CPO):

- Identified by the City Manager
- Review and approve the Analytics Infrastructure Policy (Administrative Regulation 72) and the Analytics Infrastructure Procedure.
- Approve the necessary resources required to develop, implement, maintain, test, and continually improve the analytics infrastructure framework.

3.2 Chief Data Officer (CDO):

- Identified by the City Manager
- Review and approve the Analytics Infrastructure Policy (Administrative Regulation 72) and the Analytics Infrastructure Procedure.
- Manage the overall development, implementation, maintenance, review and continual improvement of the analytics infrastructure framework.
- Conduct internal audits to ensure adherence to the analytics infrastructure policy.
- Conduct regular meetings with Business Owners and Source System Data Managers regarding data and data governance.

3.3 Business Owner:

- Identified by the department
- Primary administrative and management responsibilities for data within the department.
- Ensure data is within the scope of legal and regulatory obligations.
- Advocate the requirements of the Analytics Infrastructure Policy and the Analytics Governance Procedure.
- Ensure all staff are aware of their roles and responsibilities as defined within the Analytics Infrastructure Policy and Procedure.
- Approve and provide the necessary resources required to develop, implement, maintain, test, and improve the Analytics Infrastructure framework within the department.
- Participate in the governance meetings conducted by the CDO.

3.4 Source System Data Manager (SSDM):

- Identified by the department
- Operational responsibilities in assisting with day-to-day data administration activities.
- Provide access to departmental data.
- Act as an expert for the department's data.
- Participate in the governance meetings conducted by the CDO.

4.0 ANALYTICS INFRASTRUCTURE PROCEDURES

The procedures in this section have been established to facilitate and standardize performance monitoring and increase the accessibility of data between departments. Data elements that are developed and standardized according to these procedures will be implemented into the City's Analytics Infrastructure.

4.1 ***Identify and Inventory Data Systems.*** Led by the Business Owner, each department shall review and identify its currently available data to develop an inventory of systems that store municipal data. If not already in existence, the inventory shall be completed ninety (90) days after this regulation takes effect. Each department shall be responsible for updating its systems and the Business Owner shall provide updates during the regular governance meetings with the CDO and SSDMs.

4.2 ***Identify Relevant Business Owners and SSDMs.*** Each department is responsible for identifying individuals to fulfill the roles of Business Owner (Section 3.3) and Source System Data Manager (SSDM) (Section 3.4).

4.3 Procedures for Datasets Identified for Use by OPDA and Department Analysts

OPDA will be a primary user of other departments' data in order to fulfill its mission of improving services to the City of Cincinnati through analysis of department performance. This section outlines the steps used by OPDA, but will also apply to any other analyst or department that wishes to collaborate and share data.

There are four (4) main phases of this process:

- Identify & Authorize
- Develop
- Approve
- Implement

4.3.1 Step 1: Identify the Source System

The Office of Performance and Data Analytics (OPDA) identifies the name of the application or data that supports the operational function for performance based analysis, data discovery, and/or predictive analytics

4.3.2 Step 2: Identify the Source Database

The Chief Data Officer identifies the location of the source data.

4.3.3 Step 3: Identify the Business Owner of the Source System

The Chief Data Officer identifies the department director with administrative and management responsibilities for data within the relevant area.

4.3.4 Step 4: Identify the Subject Matter Expert(s) (SME) of the Source System

The Chief Data Officer identifies the person or group to contact for issues or questions related to the subject area.

4.3.5 Step 5: Identify the Source System Data Manager (SSDM)

The Chief Data Officer identifies the DBA or IT project manager responsible for maintaining the database of the source system.

4.3.6 Step 6: OPDA Analyst Obtains User Interface Access

With the cooperation of the relevant department, the OPDA Analyst obtains user interface access for the source system.

4.3.7 Step 7: Letter of Intent

The Chief Data Officer submits a Letter of Intent to the Business Owner to officially announce OPDA's intent to facilitate and coordinate a review of the proposed data for real-time performance monitoring (i.e., analytics). The Letter of Intent states which data OPDA will access and its purpose in accessing that data. OPDA agrees that it will utilize the data solely for the purposes described in the Letter of Intent. The Business Owner has one week to respond to the Letter of Intent with any questions or concerns regarding the review.

4.3.8 Step 8: Creation of Read-Only Profile for OPDA and the CDO

The Letter of Intent grants OPDA and the Chief Data Officer direct database read-only connectivity to the source system of the proposed data in Step 2. The SSDM will create a read-only database account to provide OPDA and the CDO access to the requested data. If restrictions are necessary to avoid disruption to production systems, the SSDM will inform OPDA and the CDO of those restrictions.

4.3.9 Step 9: Additional Agreements Regarding Sensitive Data

If the desired data contains PII or sensitive information, OPDA and the Business Owner will develop a framework for protecting that information. This may be done through anonymization (in which case OPDA will develop the algorithm to anonymize the data but the department will run the algorithm before the data is extracted and transferred), through the development of gateways and passwords, or through another method suitable to both parties.

4.3.10 Step 10: Department Completes Source System Profile

The department's SSDM completes the source system profile. OPDA's Source System Profile serves as a technical outline of the source system and database of the source system.

4.3.11 Step 11: Chief Data Officer Receives Direct Read-Only Access to the Source Data

The SSDM provides login account information for the read-only version of the source database to the Chief Data Officer.

4.3.12 Step 12: Chief Data Officer Conducts Data Analysis of the Source Database

The Chief Data Officer reviews the completed source system profile, confirms the information provided and conducts a thorough analysis of the source database. In this step, the Chief Data Officer also reverse-engineers and data profiles the relevant tables and/or views of the source database provided by the SSDM.

4.3.13 Step 13: Identify Data Elements for Extraction-Transformation-Loading (ETL)

The Chief Data Officer works collaboratively with the Subject Matter Expert(s) and Source Data Manager to identify relevant database tables and/or views that OPDA will consume for real time analysis. The data elements identified in this step originate from existing CincyStat queries and/or relevant database tables and/or views provided by the Source System Data Manager.

The department is responsible for submitting their CincyStat queries to the Chief Data Officer. This information (i.e., the CincyStat query) is required information on the department's source system profile.

If the collaboration determines new data element(s) must be established, the Chief Data Officer will work with the Source Data Manager and/or Subject Matter Expert(s) to create the new data element(s). The development of these new data elements will be documented and shared with other Business Owners to facilitate standardization among and improvement in all departments.

4.3.14 Step 14: Review & Approve Data Elements

The OPDA Analyst, Chief Data Officer, Subject Matter Expert(s) and Source Data Manager reviews the data element(s) identified in Step 11 for completeness and usage for real time analysis.

If the review calls for changes, the Chief Data Officer, Source System Data Manager and/or Subject Matter Expert(s) will collaborate to implement the required changes.

In this step, the OPDA Analyst, CDO, DSME, and SSDM also collaborate to complete the data dictionary that will be maintained by the OPDA. This step provides a way to define the structure, content and meaning of fields within the data element(s).

4.3.15 Step 15: OPDA Loads Data to the Data Warehouse

The Chief Data Officer extracts, transforms, and loads (ETL) the data element(s) to a data warehouse which is approved by OPDA (Section 2.5). The data element(s) categorized as sensitive will be protected through the process established in Step 9 to ensure compliance with all legal and regulatory obligations as they are loaded to the OPDA data warehouse.

4.3.16 Step 16: Purpose of Accessing the Data is Added to the Login Frame

To ensure individuals are using data for the purposes identified in the Letter of Intent, the Data Warehouse shall have a login screen that identifies and logs who is accessing the exported data and for which purpose the data is being used. The log-in screen should record:

- the name of the user
- the data and time of access
- the primary analysis under review/the overarching question as stated in the Letter of Intent (example: building permits)
- the specific question under investigation, which would be one of the purposes outlined in the Letter of Intent (example: components of the water permit and the average response time from the department)

The information will be recorded in a separate, password-protected location for audit purposes.