Number:	03.018.00
Last Review Date:	06/2020

City of Riverside

Administrative Manual

Effective Date:	06/2020	*Approved:*
Latest Revision Date:	06/2020	George Khalil George Khalil (Jun 10, 2020 14:03 PDT) Department
Next Review Date:	06/2022	
Policy Owner(s):	Innovation and Technology Department	Lea Deesing Lea Deesing (Jul 13, 2020 12:12 PDT) City Manager

SUBJECT:

Data Governance Policy

PURPOSE:

City-owned applications and systems, including the data stored therein, have a significant value and are an integral part of the City's infrastructure that support the City's mission, goals, and critical operations. It is essential that the City applications, systems, and data are accessed securely and are protected against information and cybersecurity-related threats and dangers.

The purpose of the Data Governance Policy is to:

- Provide consistent guidelines and procedural instructions to facilitate secure and appropriate access to City systems, and to the data used, processed, stored, maintained, shared and transmitted in and through all City systems;
- Define roles and responsibilities for data creation and usage types, cases and/or situations, and to establish clear lines of accountability;
- Develop best practices for effective data management, data sharing, and data protection;
- Enable the City of Riverside to encourage collaboration and transparency through shared data and empower users to make better data-driven decisions; and
- Ensure the protection of the City's data against internal and external threats.

POLICY:

Scope

This policy applies to all City departments, external agencies, contractors, interns, and all other persons with access to city systems and data. The policy also applies to the collection, development, and internal or external dissemination of approved data and datasets, as defined in this policy.

Definitions

Data – the statistical, factual, quantitative, or qualitative information that is regularly maintained or created by, or on behalf of, a City agency or department, and controlled in structured formats.

Dataset – a named collection of related records, often organized or formatted in tabular form or another systematic organizational format.

Data Custodian – an individual (or organizational business) unit accountable for managing information systems, technical control of data including security, scalability, configuration management, availability, accuracy, consistency, audit trail, backup and restore, technical standards, policies, and business rule implementation.

Data Owner – a business unit that primarily creates/captures and transacts with the data.

System of Records - An authoritative system where data is created/captured, and/or maintained through a defined set of rules and expectations.

Enterprise System – a computing system maintained by the Department of Innovation and Technology that is used by more than one department, and that contains operational, financial, managerial, confidential or other sensitive or mission critical information.

Geospatial fields – data or information that identified the geographic location of features and boundaries on earth and usually stored as coordinates and topology, and is a data that can be mapped.

PII and legally protected fields – personally identifiable information (PII) is any data that can be used to uniquely identify, contact, or locate a single person.

Protected data – consists of (i) any dataset or portion thereof which an agency or department may deny access, pursuant to the City Ordinance or any other state or federal law, rule, or regulation; (ii) any dataset containing a significant amount of data an agency or department may deny access, if the removal of such protected data from the dataset would impose an undue financial or administrative burden on the agency or department; or (iii) any data which, if disclosed, could raise privacy, confidentiality, privilege, or security concerns, jeopardize, or have the potential to jeopardize, public health, safety, or welfare.

Roles and Responsibilities

While specific roles/responsibilities are identified below, all City employees share in the responsibility for ensuring that City of Riverside data receives the appropriate level of protection by observing and adhering to this Data Governance policy.

City Entity / Role	Responsibilities
Chief Innovation Officer (CIO) / Data Custodian	Responsible for enterprise-wide data and information strategy, governance, security, control, policy development, and effective publication that fosters government transparency.
Data Governance Committee	Made up of existing staff from various departments and will hold quarterly meetings to identify challenges, brainstorm solutions, and discuss data needs.
Department Director / Data Owner	Head of the business unit that primarily creates/captures and transacts with the data.
Data Coordinator	IT departmental representative working under the supervision of CIO/DCIO and working with departments and external agencies to encourage safe and secure sharing of data and govern provisioning of datasets for internal and external use.
Data Steward	Department personnel designated by a department head that requests data, performs data analysis, and meets privacy and confidentiality requirements

Data Availability

Approved datasets will be made available on the City's Data sharing platform for internal and external consumption. The Innovation & Technology Department will be responsible for ensuring that the pre-approved Datasets are published as a result of this policy and are accessible from the City's central data platform.

Data Access and Usage

Access to City owned applications and systems is conditioned upon the Technology Usage and Security Policy (TUSP). Access may be revoked if either the Technology Usage and Security Policy (TUSP) or this policy is violated. All users are required to adhere to the following rules in order to use, access, store, process, and display data acquired from the City-owned applications and systems:

- Access to City-owned applications, data, and systems is granted solely to conduct legitimate business on behalf of the City.
- The accessed data must not be shared outside the scope of original request. Data should also be used according to the appropriate security or sensitivity level assigned to the data, whether used internally or externally.
- Access to specific system functions and data populations are consistent with each user's scope of employment.
- All access requests, including applications, systems, and data for internal or external use, must be submitted in writing with department head approval. The data requests must justify the need for access to the specified data. The IT department staff responsible for data security, maintenance, extract, transform, load, aggregation, data set creation, application development, etc. are preapproved and authorized to access data. Data access requests will be reviewed and approved by the department head who owns the system and the CIO, the data custodian.
- Direct access to the enterprise system of records for data analysis purpose is discouraged. Datasets for analysis and management reporting purpose will be made available upon approved requests.
- User accounts will remain active until a user's employment relationship either changes or terminates, or a dormancy period is exceeded.
- Requests to publish open data on the City's open data portal www.EngageRiverside.com must be initiated separately according to the City's Open Data Policy No. 03.016.00.
- Requests to share data with external parties or to publish on the City's open data portal will require additional review and approval by the City Attorney's Office.

Any dataset made accessible on the Data Platform shall use an open format that permits automated processing of such data in a format that can be retrieved via direct query, open application programming interface (API) and third party data analysis and reporting tools. This policy prohibits recreating a copy or subset of this dataset outside the Data Platform.

The Data Platform is not a system of record. When there is unusually high computer system input/output (I/O) activity, the City reserves the right to reduce I/O response on the Data Platform.

Department and Agency Open Data Publication

Data Platform also serves as a source to the open data publishing. In coordination with the CIO, each City agency and department shall develop a schedule for making information available to the public and updating it on a regular basis. Agencies and departments shall publish datasets with associated metadata on the City's Open Data Web Portal (in addition to other planned or mandated publication methods), and in an open format. Data Stewards are responsible for the naming, accuracy, and quality of the information. Please refer to the City's Open Data Policy No. 03.016.00 for more information.

Data Quality and Security

Data quality refers to the validity, relevancy and currency of data. All City employees must ensure appropriate procedures are followed to uphold the quality and integrity of the data they access. Where appropriate, before any internal or external data (other than publically available data) is used or shared outside the City, verification is required to ensure data accuracy and consistency will not be compromised. Data Platform records must be kept up-to-date and in an auditable and traceable manner. As necessary, data shall be retained and disposed of in an appropriate manner in accordance with the City's Record Retention policy.

Data security refers to the safety of City data in relation to the following criteria:

- Access control;
- Authentication;
- Effective incident detection, reporting, and solution;
- Physical and virtual security; and
- Change management and version control.

Appropriate data security measures must be adhered to at all times to assure the safety and security of City data. Data Platform records must be protected by appropriate electronic safeguards and/or physical access controls that restrict access only to authorized user(s). Please refer to the City's Technology Usage and Security Policy (TUSP) for more information.

Data Catalogs

The IT Department shall publish and maintain a catalog of its datasets available on the Data Platform. The catalog will be made accessible through the intranet. The IT Department will also publish a catalog of enterprise systems by placing the required catalog on the intranet and the City's web site to remain in compliance with SB272. The catalog will be updated each fiscal year.

Identification of Barriers, Guidance and Revisions

The CIO, at his or her discretion may conduct a review of existing City policies to identify impediments to open government and identify the use of new technologies. Where necessary, the CIO can propose revisions to such policies, including where greater openness can be promoted without damage to the City's legal and financial interests.

Legally Protected Information

Nothing in this Policy shall be construed to supersede existing requirements for review and clearance of information exempt from disclosure under applicable laws, regulations, ordinances, judicial orders, or other legally binding writings. Data that is confidential, protected, or exempt from disclosure under law shall not be posted through the Data Platform .

CIO Leadership

The Chief Innovation Officer (CIO), or his/her designee, will serve as the Data Governance sponsor for initiatives outlined in this Policy.

Distribution: Regular

03.018.00 - Jun2020 - Data Governance Policy

Final Audit Report 2020-07-13

Created:	2020-06-10
By:	Maria Russey (morozco@riversideca.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAsijJbxETaw91ZrnW8PrmgFBx8Bk9v608

"03.018.00 - Jun2020 - Data Governance Policy" History

Document created by Maria Russey (morozco@riversideca.gov)

2020-06-10 - 8:45:00 PM GMT- IP address: 192.248.248.55

Document emailed to George Khalil (gkhalil@riversideca.gov) for signature

2020-06-10 - 8:47:02 PM GMT

Email viewed by George Khalil (gkhalil@riversideca.gov)

2020-06-10 - 9:02:47 PM GMT- IP address: 47.148.238.49

Document e-signed by George Khalil (gkhalil@riversideca.gov)

Signature Date: 2020-06-10 - 9:03:05 PM GMT - Time Source: server- IP address: 47.148.238.49

Document emailed to Lea Deesing (ldeesing@riversideca.gov) for signature

2020-06-10 - 9:03:07 PM GMT

Email viewed by Lea Deesing (ldeesing@riversideca.gov)

2020-06-10 - 9:25:04 PM GMT- IP address: 192.248.248.55

Document e-signed by Lea Deesing (ldeesing@riversideca.gov)

Signature Date: 2020-07-13 - 7:12:54 PM GMT - Time Source: server- IP address: 172.115.110.52

✓ **Signed document emailed to Lea Deesing (ldeesing@riversideca.gov), George Khalil (gkhalil@riversideca.gov) and Maria Russey (morozco@riversideca.gov)**

2020-07-13 - 7:12:54 PM GMT