

GOVERNMENT OF THE DISTRICT OF COLUMBIA

ADMINISTRATIVE ISSUANCE SYSTEM

Mayor's Order 2017-115
April 27, 2017

SUBJECT: District of Columbia Data Policy

ORIGINATING AGENCY: Office of the Mayor

By virtue of the authority vested in me as Mayor of the District of Columbia by section 422 (2), 422 (6), and 422 (11) of the District of Columbia Home Rule Act, approved December 24, 1973, 87 Stat. 790, Pub. L. No. 93-198, D.C. Official Code § 1-204.22 (2), (6) and (11) (2016 Repl.), and the Freedom of Information Act of 1976, effective March 25, 1977, D.C. Law 1-96; D.C. Official Code § 2-531 *et seq.* (2016 Repl.), it is hereby **ORDERED** that:

I. PURPOSE

- A. This Order establishes a comprehensive data policy for the District government.
- B. The data created and managed by the District government are valuable assets and are independent of the information systems in which the data reside. As such, the District government shall:
 - 1. Maintain an inventory of its enterprise datasets;
 - 2. Classify enterprise datasets by level of sensitivity;
 - 3. Regularly publish the inventory, including the classifications, as an open dataset; and
 - 4. Strategically plan and manage its investment in data.
- C. The greatest value from the District's investment in data can only be realized when enterprise datasets are freely shared among District agencies, with federal and regional governments, and with the public to the fullest extent consistent with safety, privacy, and security. "Shared" means that enterprise datasets shall be:
 - 1. Open by default, meaning their existence will be publicly acknowledged, and further, if enterprise datasets are not shared, an explanation for restricting access will be publicly provided;
 - 2. Published online and made available to all at no cost;
 - 3. Discoverable and accessible;

4. Documented;
5. As complete as can be shared;
6. Timely;
7. Unencumbered by license restrictions; and
8. Available in common, non-proprietary, machine-readable formats that promote analysis and reuse.

D. By so sharing, the District can:

1. Improve the quality and lower the cost of government operations;
2. Make government more open, transparent, and accountable;
3. Enhance collaboration between public bodies, with partner organizations, and with the public; and
4. Further economic development, social services, public safety, and education by making data available to work with and study.

E. Because inappropriate disclosure of personal information and misuse of data for activities such as identity theft are significant concerns, the District's data must also be managed and responsibly protected. To protect the safety, privacy, and security of residents, workforce members, clients, partners, stakeholders, visitors, and others, datasets requiring protection shall be identified and:

1. Regularly reviewed to determine whether the dataset is relevant and necessary for meeting the current business needs and mission of the public body collecting the data;
2. Securely stored, transported, and otherwise technically and physically protected against unauthorized access, destruction, modification, disclosure, or loss;
3. Disseminated only to those persons and entities who reasonably require the information to perform their duties;
4. Reviewed to determine if useful derivative datasets can be created and publicly distributed by segregating sensitive portions of an enterprise dataset;

5. Reviewed to determine if metadata of derivative datasets or the combination of redacted datasets could result in the ability to accurately identify a person, and therefore jeopardize their privacy; and
6. Appropriately disposed of or archived when no longer needed.

II. SCOPE

- A. The requirements of this Order shall apply to each agency, office, board, commission, and other division of the District government ("public body") that is subject to the administrative authority of the Mayor.
- B. Each District agency, office, board, commission, and other division of the District government that is not subject to the administrative authority of the Mayor is strongly encouraged to voluntarily comply with the general standards set forth in Section I of this Order and the specific requirements set forth in Sections IV through IX of this Order.
- C. This Order does not waive of any intellectual property rights the District may have in data. Nothing in this Order grants title to any patent, copyright, trademark, or other intellectual property that the District may have in data. In an event of a conflict between any provision, term, or definition in this Order and federal or common intellectual property law, the federal or common intellectual property law shall control.

III. DEFINITIONS

In this policy, the following definitions apply:

Agency Data Officer (ADO) means an employee, designated by an agency head, who, in coordination with the CDO, helps ensure that the agency is implementing this policy.

Agency Information Security Officer (AISO) means an employee designated by a District agency head or an OCTO employee, who is responsible for coordinating with the CISO to implement, manage, monitor, and report on cyber security for their assigned agency.

Automated-anonymization-aggregation-generalization-redaction is the process of creating a new derivative dataset that can be a lower-level dataset classification for more open distribution through a straightforward and repeatable automated processes.

Chief Data Officer (CDO) means the senior official reporting to the CTO who has overall responsibility for the District's data governance processes, including the collection, creation, maintenance, documentation, dissemination, and archiving of high-quality, highly interoperable datasets.

Chief Information Security Officer (CISO) means the senior official reporting to the CTO who has overall responsibility for the District's information security strategy and practices.

Chief Performance Officer means the chief performance officer of the District government, a position within the Office of the City Administrator.

Chief Technology Officer (CTO) means the agency director of OCTO.

Creative Commons CC0 Public Domain Dedication (CC0) means a license developed by Creative Commons that allows others to freely build on, enhance, and reuse the works for any purposes without restriction under copyright or database law. Creative Commons is a nonprofit international organization that creates standard copyright licenses for use by governments and other bodies to give the public permission to share and use creative work.

Data means a subset of information, whether quantitative or qualitative, that is regularly maintained by, created by or on behalf of, and owned or licensed by a public body in non-narrative, alphanumeric, or geospatial formats. Data are an asset independent of the systems or formats in which they reside.

Dataset means a collection of data organized or formatted in a specific or prescribed way. Typically, a dataset consists of one or more tables and is stored in a database or spreadsheet. Files of the following types are not datasets: text documents, emails, messages, videos, recordings, image files such as designs, diagrams, drawings, photographs, and scans, and hard-copy records.

Dataset classification means the process of assessing the relevance of a given dataset to an agency's mission, confidentiality, sensitivity, customary availability, and legal requirements so that the appropriate level of openness and protection can be determined and applied.

Dataset classification levels are defined as the following:

- a. **Level 0, Open**, refers to all enterprise datasets that do not fall within the definitions of level 1, 2, 3, or 4. For example, certificates of occupancy are determinations by the Department of Consumer and Regulatory Affairs (DCRA) that the use of a building, structure, or land in the District conforms to zoning regulations and building codes. This dataset would not be designated by DCRA as Level 1, 2, 3, or 4 and therefore would be considered Level 0. Moreover, any dataset regularly published in machine-readable format on opendata.dc.gov or another dc.gov website prior to this Order is considered "Level 0, Open" unless an agency makes a proactive determination to raise the classification.
- b. **Level 1, Public Not Proactively Released**, refers to a dataset that is not protected from public disclosure or subject to withholding under any law (including FOIA),

regulation, or contract. Nevertheless, publication of the dataset on the public Internet and exposure to search engines would:

- i. Have the potential to jeopardize the safety, privacy, or security of residents, agency workforce members, clients, partners, or anyone else identified in the information;
- ii. Require subjective redaction;
- iii. Impose an undue financial or administrative burden on the agency; or
- iv. Expose the District to litigation or legal liability.

For example, the Board of Elections (BOE) maintains a voter file, which traditionally is public data, and in fact the BOE is required by law to “publish and display on its website ... a searchable copy of the list of qualified voters.” The law does not state that the entire file, including voter history, must be posted. Under this policy, BOE could declare the voter history to be “public but not proactively released.”

- c. **Level 2, For District Government Use**, refers to a dataset that the originating agency determines is subject to one or more FOIA exemptions, is not highly sensitive, and may be distributed within the District government without restriction by law, regulation, or contract. For example, OCTO licenses commercial data on businesses operating in the District. The license prohibits the public distribution of the data, and proprietary restrictions qualify as a FOIA exemption. Nevertheless, the data has widespread utility within the government, including for economic development and emergency management, and therefore would be classified as Level 2.
- d. **Level 3, Confidential**, refers to a dataset that the originating agency has determined is protected from disclosure by law, including FOIA, regulation, or contract and that is either highly sensitive or is lawfully, regulatorily, or contractually restricted from disclosure to other public bodies. Such datasets generally include datasets that contain data that qualifies for designation by a federal agency or District agency as:
 - i. Attorney-Client Privileged;
 - ii. Criminal Justice Information;
 - iii. Critical Infrastructure Information;
 - iv. Family Educational Rights and Privacy Act (FERPA);
 - v. Federal Tax Information (FTI);

- vi. For Official Use Only (FOUO);
- vii. Law Enforcement Sensitive;
- viii. Legally privileged;
- ix. Payment Card Information (PCI); or
- x. Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA);
- xi. Sensitive but Unclassified.

“Personally identifiable information” (PII) would generally be designated as Level 3, but not always. For example, property records contain owner names and addresses but are traditionally public data and not protected from disclosure under FOIA. On the other hand, the public library tracks the books and materials borrowed by patrons so that it can ensure the return of those assets. Disclosure of what material was borrowed by which patron(s) would violate the personal privacy of the patron and is therefore exempted from mandatory disclosure by FOIA.

- e. **Level 4, Restricted Confidential** refers to datasets for which the originating agency has determined that unauthorized disclosure could potentially cause major damage or injury, including death, to residents, agency workforce members, clients, partners, stakeholders, or others identified in the information, or otherwise significantly impair the ability of the agency to perform its statutory functions. Includes any dataset designated by a federal agency at the level “Confidential” or higher under the federal government’s system for marking classified information.

District of Columbia Internal Data Catalog (Internal Catalog) means a District government intranet-accessible web portal that is centrally managed, hosted, and funded and has capabilities similar to the District of Columbia Open Data Catalog but which is open only to District government employees and which facilitates interagency data sharing.

District of Columbia Open Data Catalog (Open Catalog) means a publicly accessible web portal that helps members of the public find, understand, and utilize enterprise datasets.

Districtwide domain tables means database tables and services designated by the CDO that provide a standard source of values to be used across District information systems and data transformations. For example, the CDO could designate a table as containing the official list of agency names and abbreviations and promote use of the table by other systems.

Enterprise dataset refers to a dataset that directly supports the mission of one or more public bodies. Typically, an enterprise dataset is stored in a named information technology system. For example, the District's general ledger is a dataset hosted in the "System of Accounts and Records." Typically, such named systems and the datasets they contain are accessible to multiple workforce members. Any named system may hold one or more enterprise datasets. Enterprise datasets include records of:

- a. **Determinations:** means final decisions, including a final decision to issue a permit or other authorization; register, certify, or license an individual or entity; impose a civil or criminal penalty; determine eligibility for a service or benefit; and award a contract.
- b. **Measurements:** means the quantification of a characteristic of an observable event, occurrence, or object in reference to a standard.
- c. **Transactions:** means a transfer, receipt, or disbursement of funds (including grants and donations) or, for example, the issuance of a purchase order.
- d. **Sensor data:** means data from devices including those deployed in the field.
- e. **Geographic data:** means spatial data for the District and its environs.
- f. **Existing digital indexes:** means the index for collections of narrative documents, videos, recordings, image files such as designs, diagrams, drawings, photographs, and scans, and hard-copy records.

Enterprise datasets also exist in small systems and spreadsheets. Any dataset, even a spreadsheet, is an enterprise dataset if it currently is maintained and:

- a. Is (or has been) used in decision making, or documents a public body's performance, determinations, transactions, or assets; and
- b. Is not largely duplicative of a dataset within an inventoried named system.

Enterprise Dataset Inventory means a listing of datasets of all public bodies, including each enterprise dataset's designated classification level and justification for that designation and other limited metadata elements for each dataset.

Freedom of Information Act (FOIA) means the Freedom of Information Act of 1976, effective March 25, 1977 (D.C. Law 1-96; D.C. Official Code § 2-531 *et seq.*). FOIA provides that any person has the right to request access to records. Under FOIA, all public bodies of the District government are required to disclose public records, except for those records, or portions of records, that are protected from disclosure by the exemptions found at D.C. Code Official § 2-534.

Information means all records, narrative and non-narrative, managed by the District.

Metadata means a description of an enterprise dataset, such as date of creation or last update; author, maintainer, or point of contact; a dictionary to support the correct interpretation of data; and documentation of methodology or business rules.

Originating agency means the District agency that compiles and manages the dataset in its original form, or on whose behalf the compiling and management is done.

Open Government Advisory Group (OGAG) means a committee of District government employees and public representatives established by Mayor's Order 2016-094, issued June 9, 2016, to provide advice on transparency, open data, and open government.

Subjective redaction means the process of creating a derivative dataset at a lower-level classification for more open distribution through a process that require humans or artificial intelligence to review the dataset each time the dataset is requested.

IV. PERSONNEL AND ROLES

A. Chief Information Security Officer

The CTO shall appoint a CISO for the District government who has the full delegated authority of the CTO for all matters pertaining to information security for the District. The CISO shall be a full-time employee who, in alignment with his or her primary responsibilities, furthers implementation of and compliance with this policy by doing the following:

1. Establishing an information security program for the District government;
2. Leading and facilitating an information technology governance program that issues detailed strategies, guidelines, standards, and policies governing the District's procurement, development, installation, configuration, implementation, use, security, and disposition of information technology systems and information;
3. Balancing security with the benefit of sharing data among District agencies, and with federal and regional partners, and the public;
4. Establishing an information technology risk management program that develops, implements, and manages a formal process for systems authorization that includes a risk assessment, the classification of data, categorization of systems, selection and implementation of controls, assessment of controls, authorization to operate, and continuous monitoring;

5. Establishing an information technology compliance program that will conduct internal District information technology assessments for compliance with laws, regulations, policies, and standards; lead the coordination of OCTO support to external information technology audits for all agencies in the District; and track all findings until remediated or residual risk is accepted by the corresponding agency Director;
6. Establishing a security engineering program that develops the security architecture for the District and designs, procures, implements, and manage information technology security appliances that provide technical security controls for the District;
7. Operating a 24/7 cyber security operations center (SOC) that monitors the District's cyber security posture across the network and all systems, detects and leads OCTO's response to security incidents, and escalates and reports on events and changes to the security baseline;
8. Expanding and operating a District identity management program that centralizes employee, contractor, and student resident identities that connects to other application databases to support physical access to buildings, government network access, government application access, and student Washington Metropolitan Transit Authority access;
9. Including the consideration for the various types of privacy data (PII, PHI, PCI, FTI, etc.) in the systems authorization process for selecting, implementing, and assessing controls, along with developing and implementing a privacy breach response and reporting process;
10. Coordinating with the CDO to promote data safeguards by the District government and safe computing practices by District government employees;
11. Establishing and chairing a committee of AISOs that propagates best management practices and meets at least quarterly;
12. Assisting the CDO in collecting, maintaining, and publishing the District's Enterprise Dataset Inventory through the systems authorization process;
13. Developing, procuring, and mandating the use of standard security tools for use by AISOs and public bodies;
14. Identifying training opportunities and in some cases providing training for AISOs and other public body staff;
15. Making recommendations to the CTO, the City Administrator, and the Mayor regarding investments to bring non-compliant public bodies or

systems into compliance with security standards, and recommending changes to laws and regulations as may be required to ensure the protection of data; and

16. Taking other actions as appropriate to further this policy.

B. Agency Information Security Officers

Within thirty (30) days after the effective date of this Order, each public body shall designate an AISO. The AISO may be an existing employee who performs other functions. The AISO is assumed to be the public body's information technology lead unless another employee is designated by the agency director. For smaller public bodies, an employee of OCTO shall, at the request of the agency director, serve as the public body's AISO, and the agency director shall appoint an employee of the public body to serve as the public body's liaison with the AISO. AISOs shall, in coordination with public body CIOs, the CISO, the CDO, and OCTO, assist with implementation of this policy by doing the following:

1. Participating in the information security governance processes for the District government;
2. Preparing, implementing, and maintaining public body security plans;
3. Conducting agency information technology system risk assessments;
4. Leading the agency information technology system systems authorization process to classify data, categorize systems, select and implement controls, and then monitor and respond to incidents as directed by the SOC;
5. Supporting OCTO information technology assessments and external information technology audits for compliance of laws, regulations, policies, and standards;
6. Balancing security with the benefit of sharing data among District agencies, and with federal and regional partners, and the public;
7. Coordinating with the CISO and CDO to promote data safeguards by the public body and safe computing practices by public body employees;
8. Participating in an interagency committee of AISOs that propagates best management practices and meets at least quarterly;
9. Assisting the CDO in collecting, maintaining, and publishing the District's Enterprise Dataset Inventory;

10. Operating information technology security systems, when appropriate, at the public body level;
11. Identifying training opportunities and in some cases providing training for public body staff;
12. Making recommendations to the CISO and agency director regarding investments to bring non-compliant public bodies or systems into compliance with security standards, and recommending changes to laws and regulations as may be required to ensure the protection of data; and
13. Taking other actions as appropriate to further this policy.

C. Chief Data Officer

The CTO shall appoint a CDO for the District government. The CDO shall be a full-time employee who, among his or her other responsibilities, furthers implementation of, and compliance with, this policy by doing the following:

1. Establishing dataset governance processes within and among District public bodies that manage data as assets, including the collection, creation, maintenance, documentation, dissemination, and archiving of high quality, highly interoperable datasets;
2. Establishing data exchange standards, including for metadata;
3. Issuing technical guidance for the publication of data by public bodies;
4. Working to ensure that data are provided to the public freely and to the fullest extent consistent with legal requirements, safety, privacy, security, cost, and efficiency;
5. Collaborating with the Chief Performance Officer to identify opportunities to increase efficiency and efficacy of government through sound data practices, analytics, and modeling;
6. Receiving and responding to public input regarding the District's data policy and activities;
7. Establishing and chairing a committee of ADOs that propagates best management practices and meets at least quarterly;
8. Designating Districtwide domain tables and promoting the use of standardized data values and elements across the District's IT enterprise;

9. Assisting public bodies in setting standards for automated-anonymization-aggregation-generalization-redaction, thereby taking datasets classified Level 1 and above and creating derivative datasets that can be classified Level 0, Open;
10. Collecting, maintaining, and publishing the District's Enterprise Dataset Inventory;
11. Developing and procuring standard tools for use by ADOs and public bodies;
12. Identifying training opportunities and in some cases providing training for ADOs and other public body staff;
13. Developing and operating systems, including the District of Columbia Data Catalog and the District of Columbia Intranet Data Catalog, that lower the cost of and increase the quality and quantity of interagency and public data sharing;
14. Working with the Chief Procurement Officer to ensure that the District's rights to and ownership of data are preserved in government contracts with particular attention to software as a service contract;
15. Establishing, with the Chief Performance Officer, a process for non-governmental actors (such as research institutions) to be vetted and access data classified above Level 1;
16. Coordinating with the Office of the Secretary regarding archive and disposition policies for data;
17. Helping public bodies prioritize the publication of datasets that are most useful to the public;
18. Publishing, in coordination with ADOs and the OGAG, an annual report to the Mayor beginning November 1, 2017. At a minimum, the report shall include recommended changes to this policy and other relevant policies, recommended legislation, a list of datasets opened during the prior fiscal year, and a list of datasets planned to be opened during the then-current fiscal year; and
19. Taking other actions as appropriate to further this policy.

D. Agency Data Officer

Within thirty (30) days after the effective date of this Order, each public body shall designate an ADO, who shall, in coordination with the public body CIO, the

CISO, the AISO, the CDO, and OCTO, assist with implementation of this policy. The ADO may be an existing employee who performs other functions. In many cases, the ADO may be an analyst with a crosscutting view of the public body's data, often an analyst who prepares performance data submissions for the Office of the City Administrator. In smaller public bodies, the ADO may be the public body's information technology or communications lead. ADOs shall further implementation of, and compliance with, this policy by doing the following:

1. Participating in dataset governance processes established by the CDO;
2. Collaborating with the Chief Performance Officer to identify opportunities to increase efficiency and efficacy of government through sound data practices and analysis and modeling;
3. Assisting with inventorying and classifying public body datasets;
4. Prioritizing public body datasets for publication;
5. Assisting in data cleanup and maintaining data quality;
6. Coordinating the publication and redactions of datasets with the public body FOIA officer and the public body's general counsel;
7. Publishing prioritized Level 0, Open, datasets on the Open Data Catalog and, as appropriate, Level 2, For District Government Use, datasets on the Internal Data Catalog;
8. Assisting the CDO with implementation of data standards and related best practices;
9. Ensuring the accuracy of the public body's enterprise data inventory listings and metadata;
10. Receiving and responding to complaints and suggestions from the public about the public body's adherence to the requirements of this data policy;
11. Assisting with automated-anonymization-aggregation-generalization-redaction, thereby taking datasets classified Level 1 and above and creating derivative datasets that can be classified Level 0, Open; and
12. Taking other actions as appropriate to further this policy.

For smaller agencies, OCTO shall, upon the request of the agency, assist the agency ADO in carrying out these functions.

V. ENTERPRISE DATASET INVENTORY, CLASSIFICATION, AND PRIORITIZATION

- A. Public bodies shall inventory their enterprise datasets.
- B. To establish the Districtwide enterprise dataset inventory, the following actions shall be taken:
 - 1. Within sixty (60) days of the issuance of this Order, OCTO shall provide public bodies with an intranet-based data inventory tool and train ADOs and AISOs on its use.
 - 2. Within one hundred eighty (180) days of receiving the tool, public bodies shall inventory and designate the dataset classification levels of their enterprise datasets using the online tool provided by OCTO. Each public body shall consult with the general counsel for the public body or the general counsels designee (and, as appropriate, other individuals necessary to determine whether the disclosure of data in the dataset may jeopardize the safety, security, or privacy of an individual or individuals) in determining the appropriate classification level of each dataset. The tool shall include a series of questions that walk public bodies through the dataset classification and the specific metadata required for each dataset. Prioritization will not be included in the initial Enterprise Dataset Inventory.
 - 3. Where enterprise datasets are not classified as Level 0: Open, an explanation for the higher classification shall be included in the inventory.
 - 4. Within two hundred and seventy (270) days of the issuance of this Order, OCTO shall publish the first iteration of the Enterprise Dataset Inventory as Level 0, Open.
 - 5. Public bodies and OCTO shall update the Enterprise Data Inventory continuously as new datasets are discovered, created, or archived.
 - 6. The enterprise inventory shall be updated annually through a process developed by OCTO. The updated inventory shall be published by November 1 of each year and shall reflect the inventory of the District's government enterprise datasets as of the prior September 30.
 - 7. By November 1, 2018, each Enterprise Dataset Inventory shall include a prioritization by public bodies for publication of Level 0, Open, datasets within the then-current fiscal year.
- C. As part of the annual dataset inventory and in coordination with public bodies, the CDO shall establish a process for assessing datasets or derivatives of datasets for

future publication as Level 0, Open. That process shall include whether publication of a dataset:

1. Would increase public body accountability, efficiency, or responsiveness, or improve the delivery of services;
2. Would help improve the public health, safety, or welfare;
3. Would provide reliable, accurate, and documented information;
4. Is already required under existing open government policies;
5. Is frequently the subject of requests from the public;
6. Is recommended by the Mayor's Open Government Advisory Group;
7. Would facilitate informed public engagement; and/or
8. Would create private sector economic opportunity.

VI. MINIMUM DATA PROTECTION STANDARDS

The safety, privacy, and security of residents, agency workforce members, clients, partners, or anyone else identified in the datasets are paramount concerns. Public bodies shall work on an ongoing basis toward meeting the following dataset protection minimum standards:

1. Public bodies shall minimize risk by limiting the collection, use, and retention of private identifying information, and its subsets such as private health information, to what is necessary to accomplish the agency's business purpose and mission.
2. Level 4, Restricted Confidential, data shall be secured via encryption, whether the data are at rest or in transit; and by additional safeguards such as digital certificates for integrity and non-repudiation. Disclosure, transmission, or dissemination of Level 4 data to other agencies within the District shall not occur unless it is approved in advance by the agency director and general counsel, and each such disclosure, transmission, or dissemination shall be documented by the AISO. Level 4 datasets shall not be accessible to the public in any way.
3. Level 3, Confidential, data shall be secured via encryption, whether the data are at rest or in transit; and by additional safeguards such as digital certificates for integrity and non-repudiation. It may be accessed and used by internal District parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized public body business must be under contractual obligation of confidentiality with the public

body before receiving it. Information identified as Level 3 or above shall not be accessible to the public in any way.

4. Level 2, For District Government Use, and Level 1, Public Not Proactively Released, data shall not be posted on the public Internet or exposed to search engines. It will, however, be made available upon request directly to the requesting entity. The data may be distributed without special security controls within the District of Columbia Intranet and between public bodies by email and other means. Whenever practical, the data shall be available through the data.in.dc.gov catalog.
5. Level 0, Open, data shall be distributed publicly pursuant to the provisions of this Order.

VII. DATA CATALOGS

A. To facilitate data sharing, OCTO shall:

1. Operate and continuously improve the District of Columbia Open Data Catalog and the District of Columbia Internal Data Catalog. At a minimum, the catalogs shall facilitate:
 - a. Searching for datasets;
 - b. Downloading of datasets in non-proprietary, machine-readable formats;
 - c. Exposing the data to developers as industry-standard application programming interfaces (API) and services;
 - d. Obtaining metadata in a consistent format;
 - e. Hosting datasets;
 - f. Managing catalog entries and data publication work flows;
 - g. Browsing by users with accessibility requirements;
 - h. Employing appropriate technology to notify users of updated datasets; and
 - i. Embedding elements of the catalog on public body websites and intranet sites;

2. Not impose incremental fees on public bodies for the publication or listing of data on the catalogs data.dc.gov, data.in.dc.gov, or opendata.dc.gov; and
3. Assist public bodies with dataset and metadata publication particularly when the process can be automated.

B. To facilitate data sharing, public bodies shall:

1. Publish all Level 0 datasets on the District of Columbia Open Data Catalog;
2. Publish Level 1 and Level 2 datasets on the District of Columbia Internal Data Catalog as appropriate;
3. Determine the frequency for updates to each dataset, and the mechanism to be utilized to update the dataset. Public bodies shall update each dataset as frequently as practical to maintain the utility of the data. To the extent possible, datasets shall be updated through an automated process;
4. If a public body is notified or otherwise learns that any dataset or portion of a dataset posted on either data catalog is factually inaccurate or misleading or is protected data, the public body shall, as appropriate, promptly correct or remove, or cause to be corrected or removed, such data from the Data Catalog and shall so inform the CDO; and
5. Not purchase or maintain data catalogs for datasets Level 2 or below other than the official Open Catalog and Internal Catalog operated by OCTO. However, public bodies should embed relevant data catalog elements on their public and intranet websites and should work to enhance the user experience for visitors to the data catalogs and agency websites.

VIII. STREAMLINED PROCESSES FOR INTERAGENCY DATA SHARING

To lower the cost and increase the speed of the intra-District sharing of datasets classified as Level 2 or Level 1, the Chief Technology Officer, in coordination with the Office of the City Administrator, shall develop uniform data-sharing agreements. A public body shall not require another public body to enter into a data-sharing agreement other than the uniform data-sharing agreement in order to have access to view, utilize, or transfer Level 1 or Level 2, datasets, unless a different data-sharing agreement is approved by the City Administrator.

IX. NEXUS BETWEEN FOIA AND LEVEL 0, OPEN DATASETS

- A. FOIA and this policy shall be distinct but complementary practices. On the one hand, FOIA request-tracking data should inform public bodies about the demand

for and priority of publishing certain datasets or derivatives of those datasets as Level 0, Open. Similarly, successful appeals for datasets previously denied under FOIA exemptions can inform public bodies about potential errors in dataset classification. On the other hand, publication of FOIA request-tracking data can help residents hold public bodies accountable for the timely and consistent processing of requests.

B. Therefore:

1. OCTO shall:

- a. Operate and improve a citywide tool for managing and tracking FOIA requests. The tool shall at a minimum facilitate request submission, request routing, and tracking responses; and
- b. Publish FOIA request-tracking data as Level 0, Open. There shall be a 14 business-day delay between closing a FOIA request and publishing data about that request as Level 0, Open.

2. Public bodies shall:

- a. Use the tool provided by OCTO (currently, <https://foia-dc.gov/palMain.aspx>) to track all FOIA requests and appeals; and
- b. Transmit responses to FOIA requests that may be publicly distributed, consistent with safety, privacy, and security, through a common portal.

X. LEVEL 0, OPEN, DATA LEGAL POLICY, AND LICENSING

The following terms and conditions are established to facilitate the sharing of datasets:

1. Nothing in this Order shall be deemed to prohibit the District from adopting or implementing measures necessary or appropriate to (i) ensure access to public datasets housed on the District of Columbia Open Data Catalog; (ii) protect the District of Columbia Open Data Catalog from unlawful use or from attempts to impair or damage the use of the portal; (iii) analyze the types of public data in the District of Columbia Open Data Catalog being used by the public in order to improve service delivery or for any other lawful purpose; and (iv) describe any modifications made to the public dataset.
2. Nothing in this Order shall be construed to create a private right of action to enforce any provision of this Order. Failure to comply with any provision of this Order shall not result in any liability to the District, including, but not limited to, OCTO or any public body or third party that establishes or maintains on behalf of the District the data catalogs required under this Order.


3. Public bodies shall not enter into agreements in which the District's data ownership or rights are transferred to a specific third party or set of third parties, unless authorized by the Mayor or the Mayor's designee.
4. The following terms and conditions apply to data publicly released by the District as Level 0, Open:
 - a. Use of click-through agreements, click-through acknowledgments, or click-through disclaimers is prohibited.
 - b. These statements shall be displayed in the District of Columbia Data Catalog and incorporated into the District's standard metadata and shall accompany each dataset:
 - i. "This data are classified by the District of Columbia as Level 0, Open. This data are placed in the public domain. The data should be treated as if covered by a Creative Commons CC0 Universal License. There are no restrictions on copying, publishing, distributing, or using the data for a non-commercial or commercial purpose. Attribution and notification to the District is not required, but is requested."
 - ii. "This data are provided as a public service, on an 'as is' basis. The District makes no warranty, representation, or guaranty of any type as to the content, accuracy, timeliness, completeness, or fitness for any particular purpose or use of any public data provided on this portal; nor shall any such warranty be implied, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose. The District assumes no liability by making data available to the public or other public bodies."
 - iii. "The District reserves the right to discontinue availability of this data at any time and for any reason."

XI. NO THIRD-PARTY BENEFICIARIES


No individual or entity shall have any right, interest, or claim under this policy or be entitled to any benefit under or on account of this policy as a third-party beneficiary or otherwise.

XII. EFFECTIVE DATE

This Order shall become effective immediately.



MURIEL BOWSER
MAYOR

ATTEST: 

LAUREN C. VAUGHAN
SECRETARY OF THE DISTRICT OF COLUMBIA