**DATA USE AGREEMENT**

**BETWEEN [Agency] AND**

**THE OFFICE OF THE CITY ADMINISTRATOR**

This DATA USE AGREEMENT (“Agreement”) is entered into between the [Agency name] (“[Agency acronym]”) and the Office of the City Administrator (“OCA”), collectively referred to herein as the “Parties” and each individually referred to herein as a “Party.”

1. The Parties

a. OCA directly oversees all executive agencies in the District that report to the Mayor. It is responsible for the day-to-day management of the District government, setting operational goals and implementing the legislative actions and policy decisions of the D.C. Council and the Mayor. As part of its operations, OCA employs The Lab @ DC, which is housed within OCA, to conduct quantitative research to evaluate and inform policy and program decisions. Staff members of The Lab @ DC are applied research scientists with expertise in statistics, experimental design, quantitative research methods, and various social science disciplines.

b. [*This paragraph should describe the functions of the data-sharing agency, with an emphasis on those functions that are related to the data that is being shared. In addition, this paragraph should reference the statutory provisions, if any, relevant to the data that is being shared.*]

2. Purpose of the Agreement

a. [*This subsection (through a series of paragraphs) should describe:*

i. *The program(s) that the agency operates that are related to the data that is being shared;*

ii. *The goals the agency and OCA seek to accomplish by sharing and using the data;*

iii. *What study, analysis, modeling, etc. will be conducted using the data; and*

iv. *The work products that will be produced; please include a pre-analysis plan if applicable*]

3. Data to be Shared by [Agency]

a. Within five (5) business days after the effective date of this agreement, [Agency] shall provide the data specified in Appendix A (hereinafter referred to as “Data”) to OCA.

*[Note: The text of section 3.a above contemplates a one-time transfer of the data. If the data is to be transferred on an ongoing basis, section 3.a will need to be revised. For example, it might state:*

* *[Agency] shall transmit the data associated with variables [list variable #s] of Appendix A to OCA once each calendar day. Each transmittal shall include the data for the prior calendar day; or*
* *[Agency] shall provide the data associated with variables [list variable #s] of Appendix A to OCA, for the time period beginning on August 1, 2015 and ending on the day before the effective date of this Agreement, within ten (10) days after the effective date of this Agreement. Following the effective date of this Agreement, the [Agency] shall provide such data to OCA for each calendar month by the fifteenth day of the subsequent calendar month.]*

b. If the Data are pulled from a database, [Agency] shall provide the exact query used to pull the Data.

c. If, during the term of this Agreement, the Parties identify additional information needed by or useful to OCA to carry out the purposes of this Agreement, the Parties may revise Appendix A by a written agreement signed by the agency representatives listed in section 15 of this Agreement.

4. Authorized Uses of Data by OCA

a. OCA shall use the Data only for the purposes described in section 2 of this Agreement.

5. Protection of Data

a. OCA shall follow the standards set forth in Appendix C in storing, accessing, and using the Data to protect the security and confidentiality of the Data.

6. Authorized Disclosures of Data

a. OCA shall disclose or provide Level 1, 2, 3, or 4 Data only to authorized users (as described in subsection b. of this section) and only to carry out the purposes of this Agreement. In addition, OCA shall only disclose or provide as much Data to an authorized user as is necessary or useful for the authorized user to carry out his or her work in fulfilling the purposes of this Agreement.

b. Authorized users are OCA employees, contractors, and agents and other employees of the government of the District of Columbia whose services OCA determines are necessary or useful to fulfill the purposes of this Agreement.

c. Before an authorized user may receive or be provided access to Level 1, 2, 3, or 4 Data, the authorized user must execute and provide to the Data Custodian a Data Confidentiality Agreement (in the form provided in Appendix B).

d. There are no restrictions on the disclosure or provision of Level 0 Data.

7. Sharing of Data for Replication Purposes

a. Notwithstanding section 6 of this Agreement, OCA may share the Data with a party outside the District government who is not an authorized user under section 6.b. if such sharing is for the purpose of validating the accuracy of analyses conducted by OCA under the Agreement (this purpose is hereinafter referred to as “replication purposes”). Level 0 data may be shared for replication purposes without restriction. In sharing Level 1, 2, 3, or 4 Data for replication purposes, OCA shall ensure that the Data is de-identified to the extent that identification is not needed for replication purposes and shall ensure that other Level 1, 2, 3, and 4 confidential or sensitive information unnecessary for replication purposes is not shared, to the extent that such sharing is not necessary for replication purposes. OCA shall also take appropriate measures to ensure that the outside party protects the Data and disposes of the Data after the Data is no longer needed for replication purposes. The sharing of Level 3 and 4 Data for replication purposes shall be approved by [Agency] in writing. In addition, the scope of the Level2, 3, and 4 Data shared with the outside party for replication purposes shall be approved by [Agency] in writing to ensure that the Data will be de-identified to the extent that identification is not needed for replication purposes and to ensure that confidential or sensitive information unnecessary for replication purposes will not be shared, to the extent that such sharing is not necessary for replication purposes.

8. Required Disclosures of Data

a. Nothing in this Agreement shall prohibit OCA from disclosing any Data if OCA is legally required to do so by judicial or governmental order or in a judicial or governmental proceeding; provided that OCA shall:

i. Notify [Agency] of the requirement to make the disclosure within forty-eight (48) hours after it becomes aware of such requirement; and

ii. Cooperate with [Agency] if [Agency] elects to contest the requirement to make the disclosure or to seek a protective order.

9. Publication of Results of Data Analysis

a. Notwithstanding section 6 of this Agreement, OCA may publish and present the results and conclusions of its analyses under this Agreement to individuals and entities outside of the OCA; provided, that:

i. The publication or presentation shall not include personally identifiable information; and

ii. The publication or presentation shall not include Level 1, 2, 3, or 4 confidential or sensitive information, unless the publication or presentation of such information is allowed under Appendix C.

b. [Optional] [Agency] will be given the opportunity to review and comment on the analysis plan. The analysis plan will be posted to the Open Science Framework (<https://osf.io>) prior to analysis of the outcome data.

c. OCA shall provide a draft of each planned publication or presentation to [Agency] for [Agency]’s review at least five (5) days before publishing or presenting the results or conclusions of OCA’s analyses under this Agreement. The purpose of [Agency]’s review is only to ensure conformity with paragraphs a.i. and a.ii. of this section.

10. OCA Data Custodian

a. OCA designates [name and title of individual] as the Data Custodian under this Agreement.

b. The Data Custodian is the OCA employee or agent who is responsible for initially receiving the Data from [Agency].

c. Once the Data is received from the [Agency] by the Data Custodian, the Data Custodian is responsible for providing the Data to authorized users and ensuring that authorized users receive access to the Data only in conformity with this Agreement (including by ensuring that a signed Data Confidentiality Agreement is signed before the Data Custodian provides access to the Data to an authorized user); maintaining a record of all Data requested and received; ensuring that the Data is disposed in accordance with section 11 of this Agreement; and providing notice of such disposition as set forth in section 11 of this Agreement.

d. Before [Agency] supplies any data to the Data Custodian, the Data Custodian shall execute and deliver to [Agency] a Data Confidentiality Agreement in the form set forth in Appendix B.

11. Disposition of Data at Termination of the Project

a. OCA shall delete Level 2, 3, and 4 Data from all places where it is stored and provide verification, in writing, to [Agency] of the manner and date of deletion within ninety (90) days after the later of the following occurrences:

i. [Agency] and OCA determine that the purpose of this Agreement has been fulfilled; or

ii. The OCA issues a final report, or other terminal work product, based on the Data.

b. The Parties may, for good cause shown, extend such ninety (90) day period in increments of ninety (90) days. Such extension must be in writing, executed by the Parties’ representatives listed in section 15 of this Agreement.

c. Notwithstanding paragraph a. of this section, OCA may maintain datasets developed from the Data so long as OCA removes any personally identifiable information and other Level 2, 3, or 4 confidential or sensitive information from such datasets.

12. Reporting of Unauthorized Disclosures or Misuse of Information

a. If the OCA discovers any actual or suspected use, access, or disclosure of Data not authorized by this Agreement, OCA shall promptly notify [Agency] in writing. Such notification shall include the following information (to the extent known by OCA):

i. The nature of the unauthorized use, access, or disclosure;

ii. The Data used, accessed, or disclosed;

iii. The individual who made the unauthorized use or access or received the unauthorized disclosure;

iv. OCA’s actions to mitigate any negative impact of the unauthorized use, access, or disclosure; and

v. The corrective action OCA has taken or will take to prevent future similar unauthorized use, access, or disclosure.

b. OCA shall be responsible for making reasonable efforts to eliminate or mitigate the negative impact of any unauthorized access, use, or disclosure of Data. OCA shall inform all unauthorized individuals who received or accessed Data that such Data was disclosed or accessed in error and of the steps the individual must take to mitigate any negative impacts of the error.

13. Data Levels

a. The Data levels (i.e., Level 0, Level 1, Level 2, Level 3, and Level 4) referenced in this Agreement refer to the data levels described in Appendix C of this Agreement*.*

14. Applicable Laws

a. [*If there are Data-specific laws that must be followed in the exchange of the Data under this Agreement, such laws should be cited here along with an acknowledgement that OCA and [Agency] will comply with such laws.*

*In addition, each specific requirement imposed by such laws with respect to the disclosure or use of the Data should be specifically listed.*]

*If there are not any Data-specific laws that apply to the date being exchanged, state that fact.*

15. Parties’ Representatives

a. The following individuals are the Parties’ representatives under this Agreement:

[Agency]

[Contact person name]

[Title]

[Address]

Email:

Phone:

OCA

[Contact person name]

[Title]

1350 Pennsylvania Avenue N.W., Suite 533

Washington, D.C. 20004

Email:

Phone:

b. All writings and notices delivered under this Agreement shall be provided to the Parties’ representatives by mail, by electronic mail, or by hand.

16. Duration

a. The period of this Agreement is from its date of execution through the date by which OCA has deleted the Data under section 10 of this Agreement (the “Termination Date”); provided, that sections 4, 5, 6, 7, 8, 10, and 11 shall survive beyond the Termination Date.

17. Modifications

a. The terms and conditions of this Agreement may be modified only upon the agreement of the Parties. A modification must be in writing and signed by the duly authorized signatories of OCA and [Agency].

18. Counterparts

a. This Agreement may be executed in counterparts, each of which shall be deemed an original and all of which shall be taken together and deemed to be one instrument.

The Office of the City Administrator and the [Agency Full Name], by the signatures of the authorized representatives below, hereby acknowledge and agree to the terms and conditions of this Agreement.

**IN WITNESS WHEREOF**, this Agreement has been executed by the Parties as of the dates set forth below.

[AGENCY FULL NAME] OFFICE OF THE CITY ADMINISTRATOR

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

By: [Name] By: Rashad Young

Title: [Title] Title: City Administrator

Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**APPENDIX A**

Dataset name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dataset security level: \_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| **Variable #1** | **Variable** | **Description** | **Notes** |
|  | Name of the field |  |  |
|  |  |  |  |
|  |  |  |  |

1. For reference, beginning with #1

*[****NOTE****: The information above should be provided separately for each separate dataset to be shared by the agency.]*

**Note Regarding Personally Identifiable Information**

If personally identifiable information—or other Level 2, 3, or 4 confidential or sensitive information—does not need to be included in the Data in order to allow OCA to fulfill the purpose of this Agreement, [Agency] shall, if possible, separate or otherwise mask such information in the Data provided to OCA. For the purposes of this paragraph, the term “personally identifiable information” is defined as information that can be used to identify, contact, or locate a specific individual (such as a name, address, social security number, driver’s license number, taxpayer identification number, email address, telephone number, financial records, educational records, health records, criminal records, or biometric information and indirect identifiers, such as an individual’s date of birth, place of birth, or mother’s maiden name) or information for which there is a reasonable basis to believe that the information can be used to identify an individual in combination with other reasonably available information.

**APPENDIX B**

**Data Confidentiality Agreement**

Pursuant to the Data Use Agreement between the Office of the City Administrator (“OCA”) and the [Agency Full Name] (“Data-Sharing Agency”), signed by the City Administrator on \_\_\_\_\_\_\_\_\_\_\_\_\_\_, 2017 and regarding the sharing of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [insert description of data shared pursuant to the data use agreement] (“Data Use Agreement”), OCA will be given access to data which includes confidential or sensitive information, such as personally identifiable information. As an authorized user of such data, I make the following affirmations:

I have carefully read and completely understand the data security guidelines outlined in The Lab @ DC Data Security Policy (the “Data Security Policy”).

I understand that I must, and affirm that I will, comply with all data security requirements specified in the Data Security Policy.

I have carefully read, completely understand, and will comply with the terms and conditions of the Data Use Agreement, including the restrictions on the use and disclosure of the data provided to OCA pursuant to the Data Use Agreement.

I understand that it is my responsibility to know the level(s) of data exchanged under the Data Use Agreement (as reported by the Data-Sharing Agency in the Data Use Agreement), and the security protections in place and necessary to ensure the protection of the data.

I will not disclose, and will take all necessary and reasonable precautions to prevent others from disclosing, any confidential or sensitive data provided pursuant to the Data Use Agreement, unless such disclosure is authorized by the Data Use Agreement.

I will not use, and will take all necessary and reasonable precautions to prevent others from using, the data provided pursuant to the Data Use Agreement for any purpose not authorized by the Data Use Agreement.

I will not attempt to use, and will take all necessary and reasonable precautions to prevent others from using, the data provided pursuant to the Data Use Agreement to contact any persons in the data for any purpose unless such contact is authorized by the Data Use Agreement.

I understand that my disclosure of confidential or sensitive information in violation of the Data Use Agreement, or my failure to abide by this Data Confidentiality Agreement or the Data Security Policy may subject me to disciplinary action, up to and including termination of employment.

I agree to report the violation or apparent violation of any term of this Data Confidentiality Agreement or the Data Use Agreement to the Data Custodian without unreasonable delay.

I acknowledge and affirm that I am personally responsible for compliance with the terms of this Data Confidentiality Agreement and the Data Use Agreement.

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

**APPENDIX C**

**The Lab @ DC Data Security Policy**

The work of The Lab @ DC (“the Lab”) often involves confidential or sensitive information. This document outlines the Lab’s procedures for working with data at all different levels of confidentiality and sensitivity and ensuring the protection of data.

# General Security Controls Employed by All Lab Staff

* All data analysis must be conducted on District-issued computers.
* All District-issued computers on which data analysis is conducted must:
* Run Windows 10 to facilitate encryption;
* Use full disk encryption (using Check Point endpoint security);
* Be password-protected; and
* Have the computer screen set to automatically lock and require a password to re-open after 5 minutes of inactivity.
* All users must use a password that is not usedelsewhere by the user and a password manager to access other analytic tools.
* All users must lock their computer screens and require a password to re-open whenever they leave a District-issued laptop unattended outside of a District government facility.
* When using a Wi-Fi connection (other than the secure Wi-Fi connection operated by the District government), all users shall comply with the following guidelines:
  + The user shall not use an unsecured public Wi-Fi connection unless such use is absolutely necessary (for example, the user’s hotel only provides an unsecured Wi-Fi connection and it is necessary for the user to perform work while at the hotel);
  + The user shall immediately connect to the DC VPN (regardless of whether the Wi-Fi connection is secure or unsecure);
  + To the extent feasible, the user shall avoid accessing or analyzing Level 3 or Level 4 data when connected to a public Wi-Fi connection, even if the user is connected to the DC VPN and even if the Wi-Fi connection is secured; and
  + The user shall ensure that his or her home network uses WPA2 authentication.

## Level 0: Open Data

**Description**: Level 0 data refers to all datasets not designated by an agency as being level 1 to level 4.

**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.

**Protections**: The Lab will not provide any protections for Level 0 data.

## Publication: There are no restrictions on the publication of Level 0 data.

## Sharing: There are no restrictions on sharing Level 0 data.

## Disposal: There are no requirements to dispose of Level 0 data.

## Level 1: Public, Not Proactively Released

**Description**: Level 1 data refers to a dataset that is not protected from public disclosure or subject to withholding under any law (including the Freedom of Information Act (“FOIA”)), regulation, or contract. Nevertheless, publication of the dataset on the public Internet and exposure to search engines would:

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

**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.”

**Protections**: Level 1 datasets may be transferred by District government email, flash drive, or the Lab’s secure upload facility. No other protections are required for Level 1 data. Level 1 datasets may be printed, but the printouts will be shredded when they are no longer needed.

**Publication**: If Level 1 datasets are used in a published document, the data may be made available with the document, but will be made anonymous and any data described in paragraphs 1-4 of the Description section above will be removed before being published.

**Sharing**: Level 1 data may be shared freely within the District government. Level 1 data will not be actively shared outside the District government directly or otherwise (e.g., by posting the data online), except as described in the Publication section above and as described in this section for replication purposes. If OCA receives a request for Level 1 data from a party outside the government, OCA will inform the data owner of the request and refer the requesting party to the data owner to request the data. If, despite the referral, the requesting party continues to request that OCA provide the data, OCA will confer with the data owner to ensure that appropriate precautions are taken (for example, subjective redactions) before the data is shared. OCA may share Level 1 data with an outside party for replication purposes. When Level 1 data is shared for replication purposes, OCA shall take appropriate steps to ensure that sensitive or confidential data is not unnecessarily shared and to ensure that the outside party appropriately protects and disposes of the data.

## Disposal: There are no requirements for OCA to dispose of Level 1 data unless specified by the data owner in a data use agreement with OCA.

## Level 2: For District Government Use

**Description**: Level 2 data 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.

**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.

**Protections**: Unless otherwise specified by the data owner in a data use agreement with OCA, Lab staff may transfer Level 2 datasets or any derivatives of Level 2 datasets by District government email, flash drive, or the Lab’s secure upload facility. However, some contracts have additional provisions that may apply (for example, the contract may require that the data must be accessed through certain interfaces). The data owner is responsible for notifying the Lab if any such restrictions exist (although the Lab intends to actively solicit this information as well) and for including those restrictions in the data use agreement with OCA. If Level 2 data is transferred via flash drive, the data will be deleted immediately from the flash drive after the transfer is complete and the deletion will be confirmed by ensuring that the data does not appear in the trash or recycle bin of the flash drive. Any Level 2 data that is printed will be stored in a locked file cabinet when the data is not in use and will be shredded when it is no longer needed.

**Publication**: The aggregate results and conclusions from OCA’s analysis of Level 2 data may be published or presented to the general public. However raw data from Level 2 datasets will not be used in a published document or a presentation unless the publication or presentation of such information is agreed to by the data owner.

**Sharing**: Unless prohibited by a contract, Level 2 data may be shared with other District government employees, contractors, and agents, but it may not be shared with an individual outside the District government either directly or otherwise (for example, by posting the data online). If OCA receives a request for Level 2 data from a party outside the government, OCA will inform the data owner of the request and refer the requesting party to the data owner. OCA will not share the data with the outside party upon such a request. If OCA seeks to share the data with an outside party (for example, for replication purposes) the sharing of the data must be approved in writing by the data owner before the data may be shared by OCA, unless such sharing is authorized by the data use agreement between the data owner and OCA. When Level 2 data is shared with an outside party, OCA shall take appropriate steps to ensure that sensitive or confidential is not unnecessarily shared and to ensure that the outside party appropriately protects and disposes of the data.

## Disposal: There are no requirements for OCA to dispose of Level 2 data unless specified by the data owner in a data use agreement with OCA.

## Level 3: Confidential

**Description**: Level 3 data 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 restricted by law, by regulation, or by contract 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:

* 1. Attorney-Client Privileged;
  2. Criminal Justice Information;
  3. Critical Infrastructure Information;
  4. Family Educational Rights and Privacy Act (FERPA);
  5. Federal Tax Information (FTI);
  6. For Official Use Only (FOUO);
  7. Law Enforcement Sensitive;
  8. Legally privileged;
  9. Payment Card Information (PCI); or
  10. Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA);
  11. Sensitive but Unclassified.

**Examples**: “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.

**Protections**: Level 3 data will only be stored and accessed on an encrypted computer. Lab staff will not email, post online, or otherwise make Level 3 data available through unencrypted channels. Level 3 data will be transferred between computers by using an encrypted flash drive or the Lab’s secure upload facility. If Level 3 data is transferred via flash drive, the data will be deleted immediately from the flash drive after the transfer is complete and the deletion will be confirmed by ensuring that the data does not appear in the trash or recycle bin of the flash drive. Any data that is printed will be stored in a locked file cabinet and shredded when it is no longer needed.

**Publication**: Unless otherwise specified in a data use agreement with the data owner, the Lab may publish and present the aggregate results and conclusions of its analyses of Level 3 data to the general public; provided that:

1. The publication or presentation of results and conclusions shall not include personally identifiable information;
2. The publication or presentation of results and conclusions shall not include raw Level 2, 3, or 4 confidential or sensitive information, unless the publication or presentation of such information is agreed to by the data owner; and
3. The publication or presentation has been reviewed by the data owner as specified by the data use agreement with between the data owner and OCA.

## Sharing: Level 3 data may only be shared with other Lab staff; OCA staff, contractors, and agents; and any individuals who are authorized to receive the data by the data use agreement between the data owner and OCA. If OCA receives a request for Level 3 data from a party outside the government, OCA will inform the data owner of the request and refer the requesting party to the data owner. OCA will not share the data with the outside party upon such a request. If OCA seeks to share the data with an outside party (for example, for replication purposes) the sharing of the data must be approved in writing by the data owner before the dataset may be shared by OCA, unless such sharing is authorized by the data use agreement between the data owner and OCA. When Level 3 data is shared by OCA, OCA shall take appropriate steps to ensure that sensitive or confidential is not unnecessarily shared and to ensure that the outside party appropriately protects and disposes of the data.

**Disposal**:Upon finishing the Lab’s work with Level 3 datasets, Lab staff will dispose of the data as specified by the data use agreement with the data owner.

## Level 4: Restricted Confidential

**Description**: Level 4 data 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 to be at the level of “Confidential” or higher under the federal government’s system for marking classified information.

**Protections**: If Level 4 data is shared pursuant to a data use agreement between the data owner and OCA, specific security protocols to ensure the protection of the data will be included in the Agreement.

**Publication**: Level 4 data may be published only if specifically authorized by the data use agreement with the data owner.

**Sharing**: Level 4 data may be shared only if specifically authorized by the data use agreement with the data owner.

**Disposal**:Level 4 data shall be disposed of in the mannerspecified in the data use agreement with the data owner.

Notes:

1. The descriptions of the data levels in this policy are based on the District’s draft Data Policy. The descriptions will be updated, if necessary, based on the final Open Data Policy.
2. The term “data owner”, as used in this policy, refers to the District agency that shared the data with the Office of the City Administrator.
3. This policy is intended only for the internal use of the Office of the City Administrator. No person or entity is intended to be a beneficiary of this policy and no person 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.