DC COURTS
Strategic Management Division
616 H Street
Washington, DC 20001

RESTRICTED DATA USE AGREEMENT BETWEEN THE DC COURTS, THE OFFICE OF THE DEPUTY MAYOR FOR PUBLIC SAFETY AND JUSTICE, AND THE OFFICE OF THE CITY ADMINISTRATOR

INTRODUCTION TO THE AGREEMENT:

DC Courts requires recipients of DC Courts data to execute and adhere to the terms and conditions of this Data Use Agreement (hereinafter, Agreement) as a condition to requesting or receiving data (Restricted or Unrestricted) from DC Courts. DC Courts agrees to provide the Requestor with data as identified in this Agreement, in return for the Requestor's agreement to use the data only for purposes that support the Requestor's study, research, or project as specifically described in this Agreement, and in compliance with this Agreement's terms and conditions protecting the integrity, security, and confidentiality of the Restricted Data described in this Agreement.

This Agreement addresses the conditions under which DC Courts will disclose and the Requestor will obtain, use, reuse, and disclose the DC Courts Restricted Data and/or any derivative file(s) that contain personally identifiable information (hereinafter, PII) or data elements that can be used in combination with other data to deduce the identity of any individuals.

This Agreement supersedes any and all agreements between the parties with respect to the use of data and preempts and overrides any prior instructions or communications from DC Courts or any of its components with respect to the data specified herein.

The terms of this Agreement can be changed by the Requestor only by a written agreement with DC Courts, executed subsequent to the execution of this Agreement and prior in time to taking any action at variance with the terms of this Agreement. Any such subsequent written Agreement between the Parties shall be denominated a modification or amendment of this Agreement, or a new superseding Agreement.

I. PARTIES TO AND EFFECTIVE DATES OF THE AGREEMENT:

This Data Use Agreement, effective as of the 18th day of August, 2017 is between DC Courts, the Office of the Deputy Mayor for Public Safety and Justice ("DMPSJ"), and the Office of the City Administrator ("OCA"), each of whom is a "Party" and who are collectively, the "Parties" to this Agreement. OCA and DMPSJ are the Requestor/Recipient/User of Restricted Data (hereinafter, "Requestor").

This Agreement shall be effective from the date this document is executed by the Parties. It may be terminated with or without cause by either Party by delivering written notice of termination to the other Party. DC Courts may, at any time and at its sole discretion for any reason, revoke the permission granted herein to the Requestor.

The Requestor shall return to DC Courts or destroy all Data once the stated use subject to this Agreement has been completed, the designated period of use has ended, or the Agreement has been terminated, whichever comes first. The Requestor agrees to destroy all electronic data files being stored at the data use site and submit in writing to the Director, DC Courts Strategic Management Division, that all electronic files have been destroyed.

II. DEFINITIONS:

"Personally Identifiable Information" (PII) is defined as information about an individual that identifies, links, relates, is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information; and information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specific individual.

"Requestor(s)" refers to the primary Requestor(s) who requests, receives, or uses data, and to his or her sponsoring or employing organization; it includes any of said Requestor's employees, agents, contractors, subcontractors, and cooperating individuals. The Requestor executes this agreement.

"Restricted Data" refers to the collection of documentation, internal memoranda, reports or data sets requested of, or provided by, DC Courts that is identifiable to any individual. Restricted data also includes any data with fields or variables that can be aggregated or combined with any other data or information to deduce any individual's identity.

"Unrestricted Data" refers to the collection of documentation, internal memoranda, reports or data sets requested of, or provided by, DC Courts that is not directly identifiable to any individual, and does not contain any fields or variables that can be aggregated or combined with any other data to deduce any individual's identity.

III. PROJECT INFORMATION AND REQUESTED DATA:

A. Project Title: NEAR Act data collection and reporting

B. Legal authority, grant, or Administrative Order if applicable: NEAR Act (D.C. Official Code 1-301-191(c)(6)

C. Data requested are (check one): _____ Unrestricted ____x____ Restricted

D. Purpose of data requested: (Please specifically identify each use of the data, to include linking to other data, publication or intended dissemination)

NEAR Act Data Collection and Reporting. Title II, Subtitle H of the NEAR Act (D.C. Official Code 1-301.191(c)(6)) tasks the Deputy Mayor for Public Safety and Justice ("DMPSJ") with preparing a report that analyzes trends in crime statistics in the District of Columbia. This report is to be submitted annually to the Council and the Mayor, beginning on December 31, 2017. The report must include information about judicial outcomes of arrests, the sentences imposed, and the prior criminal history of those who are arrested. In order to enable DMPSJ to complete this report, DC Courts has agreed to share data with DMPSJ on an annual basis. DMPSJ will use the shared data to produce the required report by linking data from DC Courts to records maintained by other federal and local agencies, including but not limited to records maintained by the Metropolitan Police Department, the Department of Corrections, and the Department of Behavioral Health. This report will then be shared with the Council of the District of Columbia, the Mayor, and, by extension, it will also be made public.

E. Will the data be used for Research, as defined in 45 CFR 46.102?

____Yes __x__No

F. Specific data elements requested (to include files, years):

DC Courts will share the following data on an annual basis, beginning on the 10th day following the effective date of this agreement and by July 31 of each subsequent year:

#	Description of data elements
1	PDID
2	Case number
3	Charge code
4	Charge description
5	Disposition for each charge
6	Sentencing data: time given
7	Sentencing data: time served
8	Sentencing data: time to serve

9	Sentencing data about supervised release (parole, probation, etc.)
10	Case file date
11	Case disposition date
12	Defendant demographics (name, age, date of birth, race, gender, address of residence) – ZIP CODE NOT ADDRESS
13	Whether there was a plea (for each charge)
14	Law/code under which each charge was brought
15	Each charge at arrest
16	Each charge at prosecution
17	Each charge at plea
18	Each charge at conviction
19	Case type (felony vs. misdemeanor)
20	Attorney is public or private
21	Diversion information
22	Judge identifier (internally unique only)- NOT INCLUDED
23	Any enhancements
24	Generated variables such as homicide, drug, etc.

The data shared will be charge-level and will include all charges regardless of judicial outcome. The initial data shared will include five (5) years of records prior to the effective date of this agreement. Each dataset subsequently shared will include the first five years of data shared, any updates to that data, and new records added since the last dataset was shared.

IV. DATA RIGHTS AND OWNERSHIP:

The Parties agree that DC Courts retains all ownership rights to the data specified herein, and that the Requestor does not obtain any right, title, or interest in any of the data furnished by DC Courts, except as authorized by this Data Use Agreement. Any use not specifically identified in III-D in this Agreement is specifically prohibited unless this Agreement is subsequently modified in writing.

V. DATA ACCESS AND STORAGE:

List the name and title of the individual responsible for receiving, maintaining, transferring, and determining final disposition of the requested data.

Name: Eric Foster-Moore
Title/Role: Data Scientist, Office of the Deputy Mayor for Public Safety and Justice

List below all individuals or organizations will be provided access to the data and the location where the data will be used/stored. (Add lines if necessary)

Individual (Last name, First name)	Affiliation and Role	Location where data will be stored
Eric Foster-Moore	Data Scientist, Deputy Mayor for Public Safety and Justice	Secure cloud server and work laptop with full disk encryption
Donald Braman	Senior Data Scientist, The Lab @ DC, OCA	Secure cloud server and work laptop with full disk encryption
Kevin Wilson	Senior Data Scientist, The Lab @ DC, OCA	Secure cloud server and work laptop with full disk encryption
Jennifer Doleac	Senior Social Scientist, The Lab @ DC, OCA	Secure cloud server and work laptop with full disk encryption
Bill Egar	Data Scientist, The Lab @ DC, OCA	Secure cloud server and work laptop with full disk encryption
Laura Heaven	Chief, Data and Performance Management, Department of Behavioral Health	Secure cloud server and work laptop with full disk encryption

VI. PRIVACY AGREEMENT:

The Requestor must initial each condition below to indicate they have read and agree to abide by the following terms:

KH A. Not to use or reuse or disclose, sell, rent, loan, lease or otherwise grant access to the Restricted or Unrestricted data in any form in any manner except as authorized in Paragraph III-D or V of this Agreement, or as authorized in a written modification/amendment to this Agreement or a new superseding Agreement.

KH B. That the requested data specified in this Agreement are necessary to achieve the Purposes described in Paragraph III-D, above.

KH C. Not to disclose direct findings, listings, or information derived from the data file(s), with or without direct identifiers, if such findings, listings or information can, by themselves or in combination with other data, be used to deduce any individual's identity. Examples of such data elements that may lead to deducing an individual's identity include, but are not limited to, name; zip code, gender; date of birth; ethnic origin; or citizenship

KH D. That any use of DC Courts data in the creation of any document (manuscript, table, chart, study, report, etc.) concerning the

purpose(s) specified in this Agreement must adhere to DC Courts' current cell suppression policy. This policy stipulates that no cell in a table that contains a number less than 20 (reflecting the number of occurrences of any compared variables) may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in a cell less than 20.

E. Not to link records included in the Restricted Data described in this Agreement to any other individually identifiable source of information, except as identified in III-D.

F. Not to identify the individuals, or provide personally identifying information about the individuals who are the subjects of the data.

G. Not to contact the individuals who are the subject of the data.

H. To assume responsibility for ensuring compliance with all the requirements for the Human Research Protection Program, as prescribed by 45 CFR Part 46, if the data requested are to be used for human studies.

I. That results of all analysis will only be presented to internal stakeholders and will not be shared publicly (such as conferences, publications, etc.) without the advance approval of DC Courts, except as specified in Paragraph III-D above.

VII. TERMS AND CONDITIONS ACCEPTED BY THE REQUESTOR:

In consideration of receiving the Restricted Data specified in this Agreement for the specific Purposes described in this Agreement, the Requestor hereby agrees to adhere to the following terms and conditions, and agrees:

A. To establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Restricted Data and to prevent unauthorized use or access to the data. MPD has reviewed and agrees that the Lab @ DC Data Security Policy (Appendix 1) establishes appropriate and sufficient safeguards to protect the confidentiality of the data shared under this Agreement, as required by this provision.

B. That the data must not be physically moved, transmitted, or disclosed in any way from the site specified in Paragraph V of this Agreement, or used for any purpose other than as described in Paragraph III of this Agreement, without the prior written approval from DC Courts.

C. To immediately report to the DC Courts Strategic Management Director and to the DC Courts signatory of this Agreement, or his or her successor or assignee, any

unauthorized use, reuse, disclosure, or loss of data files containing Restricted Data or breach of Requestor's security of the Restricted Data. "Immediately report" means within twenty-four hours of receiving a report of, or otherwise discovering or forming a belief that there has been an unauthorized use, reuse, disclosure, or loss, of Restricted Data or a potential or actual breach of Requestor's security of the Restricted Data.

D. If DC Courts determines that the risk of harm from any breach of personally identifiable information from the Restricted Data files while they are entrusted to the Request requires notification of affected individual persons of the security breach, the Requestor agrees to provide the notice without cost to DC Courts.

E. To return or destroy in a manner approved by DC Courts in writing, all original, copies, and data derived from the Restricted Data, on whatever media, at the completion of the project described in Paragraph III, or upon expiration or termination of the Agreement, whichever occurs first, within 5 days of said completion, expiration or termination, and to provide a written sworn and notarized notice to DC Courts within 5 days of destruction, attesting to said destruction and providing a description of the manner of that destruction.

F. Requestor certifies that all materials submitted with this application for restricted data are truthful.

G. Requestor acknowledges that he/she is legally bound by the covenants and terms and conditions of this Agreement, and that violations thereof may constitute unethical professional practice and/or criminal conduct and may subject Requestor and/or the sponsoring or employing organization, if any, and all his/her/its employees, contractors, subcontractors, and cooperating persons who have been identified in Paragraph V of this Agreement to the sanctions listed above, including criminal prosecution, fines and imprisonment.

H. Requestor attests that he or she is authorized to bind his or her sponsoring or employing organization, if any, and all his/her/its employees, contractors, subcontractors, and cooperating persons who have been identified in Paragraph V of this Agreement, to all terms and conditions specified herein, including terms that require Requestor to assume financial responsibility for actions inconsistent with this Agreement.

Required Disclosures of Data

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

1. Notify DCSC of the requirement to make the disclosure within forty-eight (48) hours after it becomes aware of such requirement; and

2. Cooperate with DCSC if DCSC elects to contest the requirement to make the disclosure or to seek a protective order.

VIII. MODIFICATIONS TO THIS AGREEMENT:

If any changes to information presented in III occur, the Requestor shall provide DC Courts with a copy of the revised plan and a memorandum describing the changes in advance of implementing any revisions. These revisions shall be denominated modifications or amendments to this Agreement, or a new superseding Agreement, and may not be implemented until written approval is received from DC Courts.

IX. UNAUTHORIZED USES, DISCLOSURES, OR VIOLATIONS OF AGREEMENT:

If DC Courts determines or has reasonable belief that the Requestor has made a use, reuse, or disclosure of data that is not authorized by this Agreement, or that a breach of security related to DC Courts Restricted Data has occurred or may occur, DC Courts may, at its sole discretion, and prior to any other procedures specified in this paragraph, direct the Requestor to take actions specified in this paragraph. The Requestor hereby agrees to comply with DC Courts' directions. DC Courts may direct the Requestor to: (a) promptly investigate and report to DC Courts the Requestor's findings regarding any alleged or actual unauthorized use, reuse, disclosure or alleged breach of security; (b) promptly resolve any problems identified by the investigation; (c) if requested by DC Courts, submit a formal response to an allegation of unauthorized use, reuse, disclosure or breach of security; (d) if requested by DC Courts, submit a corrective plan with steps designed to prevent any future unauthorized uses, reuses, disclosures or breaches of security; (e) and if requested by DC Courts, return Restricted Data to DC Courts or, at DC Courts' discretion, destroy the data it received from DC Courts under this Agreement in a manner that DC Courts deems appropriate.

If DC Courts determines, after a review of the Requestor's investigation, that the terms outlined in this Agreement have been violated; DC Courts will notify the Requestor of the allegation(s) and its findings in relation to the investigation in writing and will provide Requestor with an opportunity to respond in writing within 10 days. Upon review, if DC Courts deems the allegations unfounded or incorrect, the data may be returned to the Requestor under the terms of the original or a modified Data Use Agreement. If DC Courts deems the allegations in any part to be correct, DC Courts will determine and apply the appropriate sanction(s).

If DC Courts determines that any aspect of this Agreement has been violated, DC Courts may invoke these sanctions as it deems appropriate, to include, but not limited to:

A. Denial of all future access to Restricted Data files, and directed return or destruction of Restricted Data in the Requestor's possession;

B. Report of the violation to the investigator's office responsible for scientific integrity and misconduct, with a request that the institution's sanctions for misconduct be imposed.

C. If at any time DC Courts believes that criminal laws have been violated, it may refer the matter to the appropriate law enforcement authorities. If DC Courts refers a matter to law enforcement authorities, it will immediately cease providing Restricted Data to the Requestor and take such other action as may be appropriate to prevent further loss, misuse, reuse, or disclosure of Restricted Data, or breach of security, and Requestor hereby consents to cooperate fully with DC Courts' directions.

AMENDMENDED 11/9/2017:

Item III F in the original agreement signed on 8/22/2017 is amended by the requestor to add Consecutive/Concurrent to each charge sentence and the CCN number for each case.

Name of Requestor: Kevin Donahue

Title: Deputy Mayor for Public Safety and Justice and Deputy City Administrator

Organization: Executive Office of the Mayor of the District of Columbia

Street Address: 1350 Pennsylvania Ave NW, Suite 533

City: Washington State: DC Zip Code: 20001

Office telephone: 202-286-5028 E-Mail: kevin.donahue@dc.gov

Date: 11/13/17 Signature Requestor KD

Name of Requestor: Rashad Young

Title: City Administrator

Organization: Office of the City Administrator

Street Address: 1350 Pennsylvania Ave NW, Suite 533

City: Washington State: DC Zip Code: 20001

Office telephone: 202-286-5028 E-Mail: Rashad.young@dc.gov

Date: 11/13/17 Signature Requestor KD for RY

XIII. DC COURTS AUTHORIZATION:

On behalf of DC Courts, the undersigned individual hereby acknowledges that DC Courts supports the Requestor's request for and use of DC Courts Restricted Data specified in this Agreement in Paragraph III. and agrees to provide the requested Restricted Data to the Requestor in accordance with this Agreement, and agrees to make no statement to the Requestor concerning the interpretation of the terms of this Agreement and to refer all questions of such interpretations or compliance with the terms of this Agreement to the DC Courts Office of General Counsel.

The undersigned represents that he/she is authorized to enter into this Agreement on behalf of DC Courts and to agree to the terms and conditions specified herein.

DC Courts Representative: Ms. Anne Wicks

Title: Executive Officer

Date: 8/2/2017 Signature Anne B. Wicks

AMENDMENDED 11/9/2017:

Item III F in the original agreement signed on 8/22/2017 is amended by the requestor to add Consecutive/Concurrent to each charge sentence and the CCN number for each case.

Signature for Amendment

DC Courts Representative: Ms. Anne Wicks

Title: Executive Officer

Date: 11/9/17 Signature: Anne B. Wicks/cab

APPENDIX 1

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 five minutes of inactivity.
- All users must use a password that is not used elsewhere 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.

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 manner specified in the data use agreement with the data owner.

Notes:

1. 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.

2. 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.

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.