METROLAB NETWORK
DATA GOVERNANCE TASK FORCE

MODEL DATA GOVERNANCE POLICY AND PRACTICE GUIDE FOR CITIES AND COUNTIES

June 2023

Table of Contents

PREAMBLE: THE WHY, WHAT, AND HOW OF THIS GUIDE

"Data is like garbage. You better know what you are going to do with it before you collect it."
-Mark Twain

A. Purposes, Intended Uses, and Scope

1. Purposes. Data Governance is an important, complicated consideration in the modern era of local governments. As cities and counties (each sometimes hereinafter referred to as a "Jurisdiction") discover ways to use, retain, and organize data, it is imperative to learn from one another as we consider the complex nature of governance. Sharing effective approaches to policy development and implementation tools in a "community of practice" manner, as envisioned in the formation of the MetroLab Network Data Governance Task Force that produced this document, enhances the ability of local governments to both use data to provide increasingly efficient and beneficial public services, and to protect the public and mitigate risks of misuses of data.

2. Intended Uses. This Policy and Practice Guide (the "Guide") is intended to be several things:

a. A useful tool for practitioners, co-developed by practitioners (with the guidance and input of expertise from individuals from academia and other organizations with relevant expertise).
b. A living guide housed on the MetroLab Network website, and curated, updated, and refined there through a multi-functional online platform to help local governments as they keep pace with rapidly evolving Data collection and dissemination technologies and other changes in circumstance.
c. A reminder of several legal considerations that permeate Data Governance—while a few lawyers were involved in this project, it is incumbent upon us to tell you that this is not legal advice, and the local governments should of course obtain legal advice from their attorneys on legal issues affecting Data governance policies and practices.

3. Scope. The suggested governance approaches in this Guide are for Data that is owned or in possession of a city or county—this includes Data that the Jurisdiction directly collects, or Data received by a local government intentionally (i.e., the local government has contracted with a third party or is working with a third party on a project/pilot, such as a grant). While this Guide addresses a wide range of local government interactions with such Data internally and externally, it does not include governance approaches or specific policy considerations or recommendations on issues of surveillance or uses of artificial intelligence.

4. A Note on Maturity Levels: We recognize that cities and counties are at different levels of established processes with respect to Data Governance. We have included the full gamut of recommended policies. This Guide includes resources and recommendations for varied maturity levels and the website search tools will be maintained in a way designed to help users at varying stages in their Data Governance journeys navigate to the resources most pertinent to their needs and circumstances.

Simply put: got data? Use whatever portions of this Guide fit well with your needs and circumstances!

A. Data Ethics and Data Empowerment

We would like to highlight the ethos of this collaborative group of practitioners and Data Governance subject matter experts. First, what drives much of our passion and curiosity to ensure a proper governance structure is our sense of obligation to protect and provide for residents. Data is a powerful tool, a tool that is required to provide services for everyday necessities like water, electricity, and food stamps. Therefore, it is incumbent upon local governments (and other levels of government alike) to protect and take care of people's information. And while Data is something to protect, it is also something that can unlock answers to complicated challenges and improve local government services. Thus, we also wish to advocate for its (proper) use. Data is also a powerful tool *for good.* The combined importance of those two themes is the "why" behind the publication of this Guide. Local governments have a moral obligation to protect individual Data, *and* an obligation to use it to hold it accountable as a service provider. We know both can and should coexist.

B. Project History and Methodologies

1. Project History:

Origin. Students and faculty in an interdisciplinary and multi-institutional projects-based, graduate-level civic and social entrepreneurship course at the University of Missouri-Kansas City (UMKC) developed a Draft Model Data Handling Policy ("Draft Data Handling Policy") in collaboration with personnel in Kansas City, MO city government and in Kansas City, KS/Unified Government of Wyandotte County, and other individuals.[1] Many elements of that document reflected: (i) studies of data-related and "Internet of Things" (IOT) policies or guidelines in various cities in the U.S. and some in other countries, many of which were "Open Data Portal" policies; (ii) research on several issues presented by municipal data initiatives; and (iii) review of a sampling of data sharing agreements that some cities had entered into with for-profit companies and other organizations in varying contexts.

[1] The Draft Data Handling Policy was a community co-worked endeavor. Over the approximately three years of its development, student contributors to the project included several law, computer science, and engineering students across multiple semesters of an interdisciplinary Law, Technology & Public Policy course at UMKC. The UMKC faculty members principally involved as project leaders were Dr. Baek-Young Choi (from computer science), and Law Professor Tony Luppino (who, among other roles, served as lead editor). As with many other projects in the course, this project included interactions with local government staff and community engagement. Government staff significantly participating included: from the City of Kansas City, MO, Innovation Officer Bob Bennett, Innovation Analyst Kate Garman (now Kate Garman Burns), and Chief Data Office Eric Roche; and from Kansas City, KS/Wyandotte County Unified Government, Chief Knowledge Officer Alan Howze. Community members who provided input from various perspectives included James Borelli, Richard Cane, Aaron Deacon, William Mullins, Valerie Sieverling, and Bryan Wilson, collectively having relevant experiences in cybersecurity, data management, digital inclusion, insurance, law, systems engineering, and telecommunications. In addition, the Ewing Marion Kauffman Foundation supported advancement of the project through a grant to UMKC for the Legal Technology Laboratory (see www.thelegaltechlab.com), in an effort led by Prof. Luppino, Prof. Jeannette Eicks of the Vermont Law School, and Legal Technology Laboratory Program Manager John Cummins.

MetroLab Network Vetting of Draft Data Handling Policy. The Draft Data Handling Policy was vetted at a Roundtable Session at the September 2019 MetroLab Network Summit held in Boulder, CO. That session validated the proposition that many local governments were in the process of developing or were interested in developing relatively comprehensive Data Governance policies with wider scope than seen in Open Data Portal policies. It also provided great feedback and suggestions for a next iteration of that draft document that would, among other things, have more practice tools, be less "prescriptive," and offer options for local governments at varying levels of maturity in their data collection, data security and data sharing activities and processes. Following up on the Boulder session, a call for collaborators from across the United States to participate, with MetroLab network assistance, in the co-development of the next iteration of the Draft Data Handing Policy, as described in an April 2020 article in the online GovTech publication.[2]

2022 Formation of the MetroLab Network Data Governance Task Force. After a hiatus occasioned by the COVID-19 pandemic, in the winter and spring of 2022 UMKC Professor Tony Luppino renewed the call for collaborators to build on an April 2020 version of the Draft Data Handling Policy and organized an initial co-working group for its next iteration. At a Roundtable Session at the MetroLab Networks Summit in Chicago, IL in June of 2022 several members of that group presented reasons to take a "community of practice" approach to that endeavor. That session led to a collaboration, among Prof. Luppino, MetroLab Network leadership, and Miles Light of the Future of Privacy Forum to expand and formalize an initial project co-working group, which in turn resulted in the MetroLab Network formally launching a national task force to bring practitioners and subject matter experts together. That MetroLab Data Governance Task Force (sometimes referred to in this Guide as the "Task Force") is comprised of city and county staff members, metropolitan planning organizations staff members, educators, and other researchers from diverse disciplines and jurisdictions across the United States—a group of approximately 50 individuals from some 20 cities and counties that made this Guide possible.[3]

[2] *See* Cities Partner on Model Policy for Handling Municipal Data available at https://www.govtech.com/analytics/cities-partner-on-model-policy-for-handling-municipal-data.html. MetroLab Data Governance Task Force members were provided with the April 2020 Draft Data Handing Policy (on file with the editors of this Guide).

[3] This co-working effort has been greatly aided by the following Task Force members who served as facilitators of sub-groups developing content for this Guide: Ginger Armbruster, Kate Garman Burns, Sarah Carrier, Leila Doty, Abigail Eccher, Kelsey Finch, Albert Gehami, Christine Kendrick, Mahria Lebow, Jaime Lees, Tony Luppino, Jessica Nadelman, Jigyasa Sharma, and Jenna Throw. Kate Garman Burns and Tony Luppino also served as lead editors of the Guide. For information regarding the Task Force Members, see Task Force Website. The MetroLab Data Governance Task Force is composed of individuals from cities, counties, non-profits, universities, and metropolitan planning organizations from around the country. Task Force members helped provide feedback and resources that contributed to this Guide and the below-described Resources Library. MetroLab is extremely grateful for the time and contribution of the individuals listed above below. **Please note: listing of Task Force members herein or in the Task Force Website demonstrates the collaborative and comprehensive nature of this effort. It does not, in any way, indicate that these individuals or their organizations condone this Guide and should not be taken as "sponsorship," legal advice, or approval of its contents.**

2. Methodologies:

The Task Force utilized the following principal steps/methodologies in producing this June 2023 Guide:

a. Online meetings of "Sub-Groups" of volunteers to explore specific topics and "standard headaches" (i.e., "Challenges") identified in May 2022 by the initial co-working group.
b. Asynchronous postings in an online platform of comments on the April 2020 Draft Data Handling Policy, resources to consider in addressing the Challenges presented, and use cases to help guide thinking on the development of potential policies and practice tools.
c. Initial drafting of Guide text, working off of the April 2020 document as a starting place, by a group of volunteer drafters and editors from within the Task Force.
d. A series of live online co-working sessions open to all Task Force members to explore key discussion questions relating to text sections of this Guide, with results then taken into account by the editors in producing a refined draft.
e. An "all hands invited" online meeting, and an additional call for postings in the Task Force's online platform to gather feedback on that refined draft and gather "practice tools" suggestions for inclusion in the Guide or the Resources Library.
f. Presentation of the Guide in an online platform on the MetroLab website in June 2023 as both a downloadable document and electronic version that users can navigate on the site.

C. Format of this Guide

This Guide has five Sections essentially corresponding to key topic areas identified by the 2022 Initial Co-working Group and subsequently refined by the Task Force. Each Section begins with a brief "Section Note" summarizing its purpose/subject matter and noting the most prominent Challenges identified by the initial co-working group addressed in the Section, and then proceeds with recommendations of principles, policies, and/or practices a city or county might consider adopting in addressing such Challenges. It also contains several footnotes citing or linking to sources or providing other information for readers. References in the Guide to materials posted on websites mean such materials as they existed on those websites on June 20, 2023. In addition, a library (Resources Library) of Data Governance resources has been compiled in conjunction with the Task Force initiative, and contains links to a wide range of policies, practice tools, and associated background readings. Both the Guide and the Resources Library are meant to be "living" instruments accessible on the MetroLab Network website that can be updated, expanded, and refined over time. To facilitate that process, you can submit comments and suggestions on either or both by email to info@metrolabnetwork.org.

SECTION 1: DEFINITIONS AND DATA CLASSIFICATIONS

A. Section Notes

Purposes. Agreed upon definitions are key to any legal or policy regime. Definitions allow practitioners to classify technologies and standardize operations. A core set of definitions reflecting municipal uses of Data will be vital to standardizing practices across departments and jurisdictions. This Section seeks to establish definitions and Data classifications to standardize language and approaches to interdepartmental, inter-jurisdictional, and other external data sharing.

Prominent Challenges Addressed. The initial working group that led to the MetroLab Data Governance Task Force identified several scenarios, challenges, and considerations regarding "definitions" and "data classifications," including:

- Clearly distinguishing "data" from other information or facts/putting data in context.
- Addressing "hidden data" (for example, but not limited to "metadata")
- The need to have definitions and data classifications that (i) apply in various "Data Governance" scenarios, taking into account the "life cycle" of data creation, collection, storage/retention, transfer and uses, and (ii) are susceptible to consistent application.
- Complexities in endeavoring to define "Informed Consent" in the context of "opting in" or "opting out" on sharing/uses of one's data.
- Gauging the desired extent of classifications of various types of data.

B. Definitions

For purposes of this Policy, the following terms shall have the following respective meanings:

Applicable Third Party: An individual or organization, other than a Jurisdiction employee, engaged by contract or otherwise working with or for the Jurisdiction in any one or more aspects of Data Handling.

Chief Data Officer: A Jurisdiction employee designated by the Controlling Authority to perform the functions of a "Chief Data Officer" set forth in Section 5.

Community Advisory Board (sometimes herein referred to as the "CAB"): The group established and maintained to provide well-informed, timely, and independent advice to the Jurisdiction on significant Data Handling matters in accordance with Section 5 of this Policy.

Community End User Testing Group (sometimes herein referred to as the "CEUTG"): The group responsible for providing feedback regarding the use and accessibility of the Data resources, websites, applications, and other citizen interfaces, through an Open Data Program or otherwise, as described in Section 5.[4]

[4] Inspired by the Chicago Tech Collaborative's Civic Design & User Testing initiative ("CUTGroup")—see https://www.citytech.org/resident-engagement.

Controlling Authority: The individual(s), body, or other entity with the legal authority to make a decision on behalf of the Jurisdiction with regard to adopting a policy, designating an individual, body or other entity to serve a function, or other significant matter described in this Guide.[5]

Convener: The person or institution designated to lead the administration of the Community Advisory Board as provided in Section 5.

Data: A subset of information, whether quantitative or qualitative, that is regularly used by, maintained by, created by or on behalf of, and possessed, owned, or licensed by the Jurisdiction in non-narrative, alphanumeric, or geospatial formats. Data are an asset independent of the systems or formats in which they reside.[6]

Data Governance: The policies, practices, and mechanisms adopted by a Jurisdiction to manage its Data Handling.

Data Governance Oversight Committee: The committee established and maintained as such in accordance with Section 5.

Data Governance Principles: The principles set forth in Section 2 of this Guide and such other principles regarding governance of Data Handling that the Jurisdiction adopts.

Data Governance System: The processes and procedures set forth as such in Section 5.

Data Handling: The collection, creation, storage, use, transfer, dissemination, and disposal of Data, and use of Data Platforms, and related security, risk mitigation, and breach damage containment measures.

Data Intermediary: An individual or organization, other than an employee or unit of the Jurisdiction, that assists the Jurisdiction in collecting, storing, disseminating, communicating, analyzing, or disposing of Data sought for use or sharing by the Jurisdiction.[7]

[5] A jurisdiction may want to add to such a definition provision for the possibility of duly authorized "designees"—for example, if the City determined the primary authority for a decision or action normally assigned to the Controlling Authority should be the Mayor, the City Manager, or the City Council or similar body, but such Controlling Authority has discretion to delegate such authority, there could be language included in the definition along the lines of "or the designee to which such authority duly assigned responsibility for the particular decision or action in question."

[6] Based largely on the corresponding definition in District of Columbia Data Policy available at https://octo.dc.gov/page/district-columbia-data-policy.

[7] There are many examples of definitions of the term "Data Intermediary" in various contexts. *See, e.g.,* Civic Switchboard Guide, *Defining a data intermediary* at https://civic-switchboard.gitbook.io/guide/context-and-concepts/defining-a-data-intermediary; *How to know you are a 'data intermediary" under the Data Governance Act*, posted April 27, 2021 on the International Association of Privacy Professionals (IAPP) website at https://iapp.org/news/a/how-to-know-you-are-a-data-intermediary-under-the-data-governance-act/ (in the context of European Union then proposed regulation); The one included in this Guide is for purposes of describing a role to be taken into account in Data Governance recommendations offered herein.

Data Security Policy: The "Data Security Policy" described in Section 3.B.2.

Dataset: 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.[8]

Data Platform: The methods, machinery, software, and related tools and systems utilized by the City or Applicable Third Parties to collect, store, use, or make public any Dataset, including, without limitation, those utilized in any Open Data Program.

De-Identify: To remove all Personally Identifiable Information from Data.[9]

Encrypted: Any Data format with content designed to be protected and accessible only by private parties specifically intended as an audience.

Machine-Readable: Any Data format in which a computer can read and process information.

Open Data: Data made open and freely available to all online in a Machine-Readable, open format that can be easily retrieved, downloaded, and reused utilizing readily available and free Web search applications and software.[10]

Open Data Program: A City program dedicated to making specific Datasets available as Open Data to the public, including, without limitation, programs that engage civic technologists, the research community, and other partners to make use of such Datasets in support of the program's goals.[11]

Open Data Programs Manager – The Jurisdiction employee designated by the Controlling Authority to manage the City's Open Data Programs and to perform the functions pertaining thereto described in Section 5.

[8] *Id.*

[9] Some jurisdictions may want to adopt a more robust definition, such as the following from the California Consumer Privacy Act ("CCPA"): "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a businesses that uses de-identified information: 1. Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. 2. Has implemented business processes that specifically prohibit reidentification of the information. 3. Has implemented business processes to prevent inadvertent release of de-identified information. 4. Makes no attempt to re-identify the information.

[10] Based on Current Kansas City Policy, Section 2-2130 KC, in Chapter 2 of its Code of Ordinances at https://library.municode.com/mo/kansas_city/codes/code_of_ordinances?nodeId=PTIICOOR_CH2AD_ARTXVIOPDAPO ("KCMO Open Data Policy").

[11] Based in part on definition of "City of Seattle Data" in Seattle's Open Data Policy V1.0 (Feb. 16, 2016) available at https://www.seattle.gov/Documents/Departments/SeattleGovPortals/CityServices/OpenDataPolicyV1.pdf (hereinafter "Seattle Open Data Policy").

Payment Card Industry (PCI) Data Security Standard: Standards adopted by the Payment Card Industry Security Standards Council to protect payment information for safe financial transactions.[12]

Personally Identifiable Information ("PII"): information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual (sometimes shortened to "personal information"). Examples include but are not limited to:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- Biometric information.
- Internet or other electronic network activity information including but not limited to, browsing history, search history, information regarding an individual's interactions with a government website or application.
- Geolocation data.
- Audio, electronic, visual, or similar information.
- Professional, educational, or employment-related information.
- Inferences drawn from any of the information identified in this subdivision to create a profile about an individual reflecting their preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes.

***Note**: Cybersecurity insurance or other policies may have different definitions of PII that could impact policies and processes.*

Principal Data Handling Administrator: The Chief Data Officer or other individual designated by the Controlling Authority to be primarily responsible for oversight of adherence to this Policy.

Privacy Laws: All laws containing provisions for the protection of a person's privacy by regulation of the collection, storage, use, and/or release of any PII of such person.

Public Disclosure Law(s): All open meetings, open records, public records, freedom of information, or similar laws pertaining to disclosure, notice, or other transparency requirements to which any Data Handling activities of the Jurisdiction are subject.

Re-Identify: To convert anonymized or De-Identified Data into PII.

[12] *See https://www.pcisecuritystandards.org/standards/*

Sensitive Data: Information that the Jurisdiction determines should be safeguarded and protected against unwarranted disclosure for legal or ethical reasons, for reasons pertaining to personal privacy, or for proprietary considerations, and includes, without limitation, PII.[13]

Unit Data Steward: The Jurisdiction employee designated by the Chief Data Officer as the person in a Jurisdiction agency or department responsible for performing the functions of a "Unit Data Steward" described in Section 5.

C. Data Classifications Recommendations

Note: *The following Data classifications recommendations in this subsection assume that the Jurisdiction's Data Handling experience is fairly mature. An alternative set of recommendations for Jurisdictions with less mature Data Handling experience is presented at* Alternative Data Classifications For Less Mature Data Handling Systems. *See also other resources regarding Data classifications in the Data Classifications section of the* Resources Library.

If Data is not already classified by a third party, cities and counties should establish Data classifications by level of sensitivity. Sensitivity levels inform data collection, retention, storage, dissemination, and disposal. Classifying data protects privacy, limits data misuse, maximizes data usage, and facilitates sharing of open data sets. The following suggested classifications could be established by rule or practice and incorporated into training, security measures, and data-related decision-making. Data classifications should be reviewed regularly and updated as necessary. These classifications will also inform the parameters of a local government's Data Security Policy.

Level 0—Open
Any Dataset regularly published in Machine-readable format by Jurisdiction or its Units on the Jurisdiction's website, or otherwise treated as Open Data is considered "Level 0—Open" unless the Jurisdiction or a Unit makes a proactive determination to raise the classification.

Level 1—Public, Not Proactively Released
Data available for public access or release, not subject to any restrictions under any Public Disclosure Law or Privacy Law.

Level 2—For Internal Government Use
A Dataset that the Jurisdiction determines is subject to one or more Public Disclosure Law exemptions, but is not highly sensitive, and may be distributed within the Jurisdiction government without restriction by law, regulation, or contract. Data that is normal operating information but is not proactively released to the public. Viewing and use is intended for employees; it could be made available Jurisdiction-wide or to specific employees in a department, division, or business unit. Certain data may be made available to external parties upon their request.

[13] Based largely on definition of Sensitive Data University of North Carolina University Libraries Data Security: Policies and Regulations Impacting Research Data: Definition at https://guides.lib.unc.edu/datasecurity/definition#:~:text=Sensitive%20data%20are%20defined%20as,be%20protected%20against%20unwarranted%20disclosure .

Level 3—Sensitive
Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.

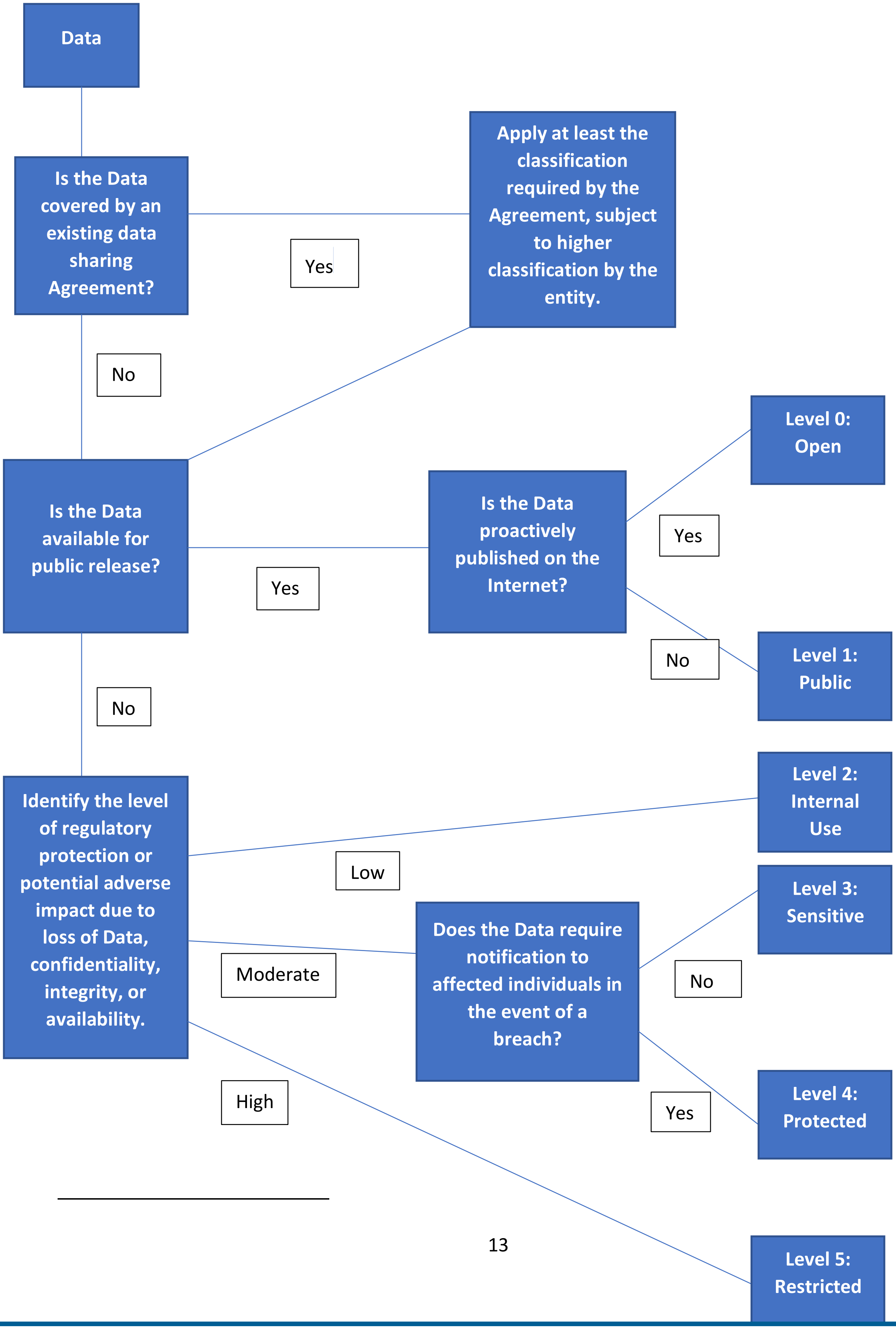
Level 4—Protected
Data that triggers a requirement for notification to affected parties or public authorities in case of a security breach.

Level 5—Restricted
This data poses direct threats to human life or catastrophic loss of major assets and critical infrastructure (e.g., triggering lengthy periods of outages to critical processes or services for residents). Before classifying data as Level 5 Restricted, you should speak with leadership in your Unit and the Jurisdiction's Chief Data Officer.[14]

A Data classification flowchart and examples of each category of Data follows below:[15]

[14] Modeled after Washington D.C. approach at https://opendata.dc.gov/pages/data-policy#definitions and San Francisco approach at https://sf.gov/sites/default/files/2021-05/DataClassificationStandard_FINAL_0.pdf.

[15] Inspired by San Francisco's Data Classification approach at https://sf.gov/sites/default/files/2021-05/DataClassificationStandard_FINAL_0.pdf.


Data
Is the Data covered by an existing data sharing Agreement?
Yes
Apply at least the classification required by the Agreement, subject to higher classification by the entity.
No
Is the Data available for public release?
Yes
Is the Data proactively published on the Internet?
Yes
Level 0: Open
No
Level 1: Public
No
Identify the level of regulatory protection or potential adverse impact due to loss of Data, confidentiality, integrity, or availability.
Low
Level 2: Internal Use
Moderate
Does the Data require notification to affected individuals in the event of a breach?
No
Level 3: Sensitive
Yes
Level 4: Protected
High
Level 5: Restricted

Data Classification Examples

Data classification	Examples
Level 0 Open	• Open Data • Public websites • Press releases • Job announcements • Public reports • Bid/contract/RFP announcements
Level 1 Public, Not Proactively Released	• Certain financial data and reports • Health or building inspection information • Notices about future construction projects • Organizational charts • Internal memos
Level 2 Internal City Government Use	• Employee phone directory • Draft reports, memos, and meeting minutes • Internal project documents • Intranet • Fuel consumption/fleet management data • Learning management data • Some financial data • Some audio and video recordings • License plate numbers

Level 3 Sensitive	• Personnel records (including employee name + employee number, performance appraisals) • Personally identifiable information (PII) not triggering statutory notification requirements • Certain public safety/criminal record data • Sensitive Security Information (SSI) • Physical security access logs • Investigative data (e.g., related to citations, legal proceedings) • Trade secrets/proprietary/commercially sensitive data • Internal risk management and mitigation data • Central property management information • Browser history • Privileged communications • Biometric information
Level 4 Protected	• Social security number • Driver’s license number • State ID number • Payment Card Industry (PCI) data and other customer financial information • Protected health information (PHI) •Password and PIN numbers •Student records (FERPA) • Federal tax information • Some criminal justice information
Level 5 Restricted	• Certain network/infrastructure information • Certain water infrastructure • Some emergency response information • Some data obtained from federal government

SECTION 2: PRIVACY AND OTHER DATA GOVERNANCE PRINCIPLES

A. Section Notes

Purposes. This Section offers recommendations on privacy protection principles as well as other Data Governance core principles and discusses the role of resolutions in establishing such principles.

Prominent Challenges Addressed. The initial working group that led to the MetroLab Data Governance Task Force identified several categories of challenges and considerations relating to privacy protection and other principles for city or county Data Governance, including:

- Ensuring focus on both constituent right to privacy and constituent right to data protection.
- Mindfulness of both "consumer protection" principles traditionally associated with activities in for-profit commerce and the public service responsibilities of cities and counties.
- Staying up to date with requirements of the Freedom of Information Act (FOIA),[17] public disclosure/open records and other transparency/disclosure laws and dealing with tensions between those and privacy laws and "preemption" issues.
- Being mindful of international rules/standards, such as the European Union's General Data Protection Regulation (GDPR)[18]
- The need to establishing clear equity and ethics principles and guidelines that can be operationalized and consistently applied.
- The value of embracing "Data minimization"—collecting only what's needed.

B. Privacy Principles and Resolutions

"Rules are not necessarily sacred, principles are." – Franklin D. Roosevelt

Privacy is an essential component of Data Governance. It is the right that determines the protection of an individual's information.[19] Depending on the level of data governance maturity and resources, there are three approaches to building in privacy as a key Data Governance pillar:

(i) Establishing privacy principles by way of resolution.
(ii) Conducting privacy impact assessments.
(iii) Establishing privacy policies.

1. Privacy Principles.

While cities, counties and states use many rules and regulations, a common first step is to establish privacy principles, often by way of resolution passed by the Jurisdiction's governing body. Beginning

[17] *See* https://www.foia.gov/.

[18] *See* https://gdpr.eu/.

[19] *See* the definition of "Privacy" in the online version of Black's Law Dictionary (2ND Ed.) at https://thelawdictionary.org/privacy/: "The right that determines the nonintervention of secret surveillance and the protection of an individual's information."

in 2015, cities started publishing privacy principles to help establish trust with the community and express a commitment to using data for good and seeking to avoid unintended consequences. Or, as Columbus, Ohio says it, "the Data Privacy Plan starts with a statement of principles that illustrates Smart Columbus' commitment to the ethical use of data.

For a comparative look at (simplified/edited) city privacy principles, please see the below table:

Portland, OR[20]	Kansas City, MO[21]	Columbus, OH[22]
Transparency: managing and collecting information in a described way clearly, accurately, and shared in an accessible way.	Kansas City values privacy and considers risks to the well-being of the public before collecting, using, or disclosing personal information.	Smart Columbus is as open to the public as it can about how it collects personal data.
Data will be secured and protected throughout its lifecycle.	The City will only collect information that is needed to deliver city services, and the data will be kept only as long as legally required or valid for a business purpose.	Smart Columbus will notify individuals when it collects their information.
Prioritization of the needs of marginalized communities regarding data and information management.	When appropriate, the City will disclose how personal data will be used and give the option to choose how it is used whenever possible.	Smart Columbus will use an individual's information only for the purposes stated in the notice, and to which the individual consented.
Fair stewardship of data and information with non-discriminatory protections and understanding impacts of unintended consequences.	The City will restrict improper access to data, securing cyber systems and storage resources.	Smart Columbus projects will collect only the minimum amount of personal information that they need to accomplish their purpose.
Third parties working with city data must not expose confidential or private information.	Business partners and contracted vendors who collect or receive personal data must agree with city privacy requirements.	Smart Columbus will apply robust information security controls that take into account the sensitivity of project data

[20] Available at https://static1.squarespace.com/static/5967c18bff7c50a0244ff42c/t/5d0aec446939ce00011ec049/1560996933477/COP_PIP_handout_June19_2019.pdf.

[21] Available at http://www.communityofreasonkc.org/wp-content/uploads/2016/06/Data-Privacy-Principles.pdf.

[22] Available at https://smartcolumbus.com/about/privacy-policy.

		and the risk of individuals that it poses if released.
The City will create procedures for reviewing, sharing, assessing, and evaluating automated decision system tools around equity, fairness, transparency and accountability.	Residents should have an effective and responsive mechanism for exercising privacy complaints. The City will receive, investigate, and respond to individuals' complaints.	Smart Columbus will ensure that the data it releases on the Smart Columbus Data Portal does not contain information about identifiable individuals.
All data must bring value to the City, the City will collect only the minimum amount of personal information to fulfill a well-defined purpose.		Smart Columbus will institute the processes necessary to ensure that it follows and meets each above principle.

For examples from other Jurisdictions, see the Privacy Principles section of the Resources Library.

While the language varies, there are consistent themes across city and county privacy principles. These themes include:

- Minimal and intentional collection of Data: the best form of Data protection is at the onset.
- Transparency and notice: when possible, describe for what purpose the Data is being collected.[23]
- Equity: consider the collection of key demographic Data and the relationship to race and social justice efforts.
- Ethical and non-discriminatory use of Data: Data is used only for its intended and described purpose.
- Data openness: maintaining transparency on the type of data collected and when appropriate, publishing on open Data.
- Cyber security: ensure the protection of Data.
- Contracting with outside parties: consider privacy protections and transparency requirements for third parties.
- Ongoing accountability: put measures into place that allow for regular accountability.

Key takeaway: Privacy principles are a way to establish a commitment to privacy values that will provide guidance and parameters as the Jurisdiction moves forward in developing its privacy practices. Use these central themes as a guiding list to consider and employ best practices for community engagement described in Section 5.

[23] *Cf.* NYC Guidelines for the Internet of Things at https://iot.cityofnewyork.us/privacy-and-transparency/ (Privacy + Transparency).

2. Privacy Impact Assessment.

Another way to protect resident privacy is to build a privacy review into IT processes by conducting privacy impact assessments. The following language comes from the City of Seattle, WA:[24]

"A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. It asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access."

The centralized IT department asks questions of the department seeking to procure the specific technology. Questions addressed in these assessments include some of the following:

- Describing the purpose and benefit of the technology.
- Who is using the technology?
- What legal standards or conditions must be met (e.g., for criminal justice data systems, etc.).
- What information is being collected?
- What measures are put in place to minimize inadvertent or improper collection of data?
- Who can access the data collected?
- If operated or used by another entity than the jurisdiction, link the memorandums of agreements.
- How will data be stored? What is the data retention policy?
- How will the department owner consider the audit process to maintain compliance?
- Explain how the technology/project checks the accuracy of the information collected?
- Describe what privacy training is provided to users?

Regularly asking departments to understand these detailed aspects of technology and data use allows for a thorough analysis of privacy risks.

For other sources of guidance on Privacy Impact Assessments see the Privacy Impact Assessments section of the Resources Library.

3. Privacy Protection Resolutions.

In addition to privacy principles, Jurisdictions can consider resolutions that support privacy-forward processes. This includes:

[24] Available at https://seattle.gov/tech/initiatives/privacy/privacy-reviews.

- When feasible, the Jurisdiction shall provide public notice available to the affected person about the collection, use and sharing of personal information at the time of collection. This includes instructions about opting out of this collection, whenever reasonably feasible.[25]
- Facilitate informed consent[26] when information imputing a privacy interest of the citizen is collected or disseminated. Informed consent refers to a person's agreement to allow PII or other personal Data to be provided for research, reporting, and statistical purposes after being apprised of all material facts the person needs know in order to make the decision to provide such agreement intelligently, including awareness of any material risks involved, potential uses and users of such Data, and of alternatives to providing or allowing the collection of such Data.
- Adhere to the Data retention schedule recommended from time-to-time by the Data Governance Oversight Committee or recommended or mandated by applicable laws and ordinances and approved by the Controlling Authority and dispose of or De-Identify information as required by such retention schedule.
- Maintain public documentation explaining privacy practices that are in compliance with its privacy principles and policies.
- Provide individuals with the opportunity to correct Data inaccuracies.[27]

In addition to these processes, consider when additional notice should be given when Data is shared *internally* to a Jurisdiction. For example, if a parks department gives Data to a policy department, a new data use or shift in resident expectation (that wasn't shared at the onset of data collection) has potentially occurred. Intentionality should be at the core of Data collection. Jurisdictions often fail to address the "why" of Data collection. Data minimization is key to protecting residents' privacy rights; accordingly, being intentional about why and how resident Data is collected is of paramount importance. Municipalities should standardize Data collection requirements and justification for the same. In considering the recommendations offered in this Section 2 and in Section 3, one should be mindful that there are three conditions that justify data collection:

(i) Mandated by law.
(ii) Requirement imposed by an external funder of a program.
(iii) Required to ensure optimal allocation of resources.

In addition to considering a resolution, staff can develop internal core principles for a Jurisdiction's leadership and staff to exercise appropriate care and diligence. Some suggested internal principles:

- As stewards of data, we aim to protect and preserve the digital and physical environments.

[25] *Cf.* REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation-"GDPR"). Paragraph 32, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[26] Many commentators have suggested that consideration be given to the development of better approaches to meaningful informed consent to the capturing and use of personal data—i.e., beyond clicking "accept" to complex/dense descriptions in terms of use. Reviewers of this Guide are encouraged to email to info@metrolabnetwork.org suggestions and references to resources pertinent to this challenge.

[27] *Cf.* Seattle Open Data Policy at
https://www.seattle.gov/Documents/Departments/SeattleGovPortals/CityServices/OpenDataPolicyV1.pdf.

- We aim to foster a culture that recognizes responsibility and duty to do so rests on the shoulders of government, residents, citizen groups, educational organizations, and businesses alike.
- We shall maintain ethical standards and maintain compliance with all local, state, and federal privacy laws that preserve and protect Data.
- We understand the importance of Data Governance starting at the point of collection – aiming to minimize the collection of PII whenever possible.
- Whenever possible, we shall provide the possibility for an individual to exercise the right to "opt out" or exercise the right not to have their PII disclosed or sold absent consent lawfully provided on their behalf by an authorized person.[28]
- We will emphasize and maintain transparency with the public on the usage and collection of data where it is prudent and reasonable.[29]

C. Other Data Governance Principles and Resolutions

"The basis of our governments being the opinion of the people, the very first object should be to keep that right; and were it left to me to decide whether we should have a government without newspapers, or newspapers without a government, I should not hesitate a moment to prefer the latter. But I should mean that every man should receive those papers and be capable of reading them." - Thomas Jefferson (Letter to Edward Carrington, January 1787)

As discussed in the Preamble to this Guide, in addition to protection of Data privacy, the Task Force embraces the use of Data by cities and counties to address complex challenges and improve government services. Moreover, as addressed in Section 5 of this Guide, local government can and should engage the communities they serve in well-informed ways to collectively leverage properly available data for public good. Accordingly, in addition to the Privacy Principles and Resolutions discussed in Subsection B. above, it is recommended that Jurisdictions consider adopting by resolution principles along the following lines:

- The Jurisdiction is committed to maintaining a robust, dynamic, and easily accessible Open Data Program to both (i) serve the public's right to public information and (ii) facilitate community engagement and collaborative civic innovation in the delivery of public services and in actions that enhance the quality of life and opportunities for prosperity for residents and organizations and protect the physical environment in which they reside.
- The Jurisdiction shall employ Data management and Data governance practices designed to ensure that Data it seeks to use is of sufficient integrity and is accessible to appropriate parties

[28] Based on "opting out" provisions in The California Consumer Privacy Act of 2018-see https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[29] Based in part on City of Charlotte, Open Data Policy Jan. 1, 2015, at page 1, available through https://charlotte.maps.arcgis.com/home/item.html?id=7c88b8633b034ddcbbd6badb1b7076fe. See also NYC Guidelines for the Internet of Things at https://iot.cityofnewyork.us/privacy-and-transparency/ (Privacy + Transparency).

in proper and efficient ways that facilitate informed decision-making in pursuit of fulfilling its duties to the public and implementing its strategic plans for public benefit.

The Task Force has identified various resources supporting the value of a Jurisdiction adopting those two principles and containing descriptions of practices to implement them that users of this Guide are encouraged to consider—*see the Open Data Policies section of the* Resources Library.

In particular, we wish to highlight Washington DC's data policy reflecting the intentional effort of using Data as a tool to improve services.

From "Purpose" in D.C. Data Policy:[30]

> "3. 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.
>
> 4. 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."

[30] *See* "D.C. Data Policy" at https://opendata.dc.gov/pages/data-policy#legalpolicy. *Cf.* KCMO Open Data Policy at Section 2-2132, stating: "(a) Whenever possible, technology shall be procured and efficient processes shall be used in a way that advances the policy of making public data and information open and available through the use of open data standards and formats. (b) To the extent prudent and practical, public data shall be published online and made freely available to all in a machine-readable open format, in both its raw and processed form, including a description of the source and quality of the data, all of which can be easily retrieved, downloaded, indexed, sorted, searched, analyzed and reused utilizing readily-available and free web search applications and software."

SECTION 3: DATA INTEGRITY AND DATA PROTECTION/CYBERSECURITY

A. Section Notes

Purposes. Doing public good with Data requires that the Data is of sufficient quality/integrity, is properly accessible, and is stored safely. Recent cybersecurity incidents faced by city and county governments very clearly highlight the importance of strong information security and privacy preserving practices when governments collect sensitive personal information. This Section 3 offers recommendations regarding data quality/integrity and data protection and security standards and practices, as well as measures to lessen risks of damage from data breaches or cybersecurity attacks, in relation to intra- and inter-departmental data processing activities. Note: various levels of designated Data classifications require different and unique process considerations. Please refer to Section 1 for recommendations regarding Data classifications.

Prominent Challenges Addressed. The initial working group that led to the MetroLab Data Governance Task Force identified several scenarios, challenges, and considerations in connection with Data integrity, Data Protection, and cybersecurity, including:

- Adopting measures to promote sufficient "quality" of useable Data.
- "Data Minimization" (collecting only what's needed).
- Being mindful of international rules/standards (e.g., the EU's GDPR)
- Employing approaches to risk assessment that keep pace with emerging technologies (e.g., on risks of "re-identification" through aggregation of multiple "anonymized" datasets)
- Having clear policies and practices on storage and retention.
- Establishing Data security and network security measures/standards/protocols.
- Utilizing processes/checklists for dealing with "incidents" and "breaches."

B. Quality and Security Measures, Compliance, and Audit Mechanisms

Note: cybersecurity is a complex endeavor with several processes to consider. This section is a high-level overview, with auditing being a particularly key tool to ensure cybersecurity measures are in place.

1. Data Quality and Integrity.

"Data Quality" is critical to avoid garbage in garbage out. Once data is acquired, every data pipeline should go through a Data quality check. A Data quality check includes assessment of Data accuracy, validity, timeliness, and completeness. Jurisdictions can set up review processes and steps to assess Data quality. Baseline Data assessment should include the following:

- Completeness – check for empty/null value or missing values.
- Uniqueness – check for duplicate values.
- Accuracy – check for anomalies such as a string value in a numeric dataset or vice versa.
- Timeliness – check Data frequency (collected daily, weekly, monthly etc.) and ensure that it is up to date.

As capacity allows, Jurisdictions can embed the baseline quality checks and other auxiliary tests in the acquisition process itself. Datasets that fail baseline assessment should trigger a warning to the Data owner and initiate a review and correction process.[31]

"Data Integrity" goes beyond Data Quality which is primarily limited to checking for errors or anomalies in the dataset. Ensuring Data Integrity requires ensuring (to the best of your ability) that the Data is internally consistent and as free of bias as possible.[32]

2. Data Security Policy.

The Jurisdiction should adopt a formal, written **"Data Security Policy"** for establishing and communicating Data security requirements across all Jurisdictions departments and agencies. The Data Security Policy should:

a. Classify all Data provided to, collected by, or derived by the Jurisdiction or its representatives. See Section 1.C for guidance on Data classification.

b. Establish separate criteria for access to and use, modification and deletion, reproduction, disclosure, and storage and retention of each classification of Data.

c. Establish mechanisms for controlling and managing the access to and use, modification and deletion, reproduction. disclosure, and storage and retention of all Data according to its classification criteria.

d. Establish indicators and measurements to monitor compliance with the provisions of the Data Security Policy and detect unauthorized access and malicious use in violation of the Data Security Policy.

e. Require position-appropriate Data security training for (i) all Jurisdiction employees and (ii) all personnel of Applicable Third Parties who will be handling Sensitive Data.

f. Maintain plans to remedy or mitigate violations of the Data Security Policy and plans to respond to system failures and breaches.[33]

g. Require periodic audits of all Data Handling control and management mechanisms to ensure compliance with the Data Security Policy.

[31] For an example of a "Data Quality Self-Assessment Checklist," see NYC Open Data – Data Quality Standards and Review Process (May 2022 Revision) at pages 5-6, available at https://docs.google.com/document/d/1hnmsJDkI4YmO8Pzk2yljFouwCFbdfbIfSn65Re074HU/edit.

[32] *See, e.g.,* Brookings report Algorithmic bias detection and mitigation: *Best Practices and policies to reduce consumer harms* at https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/ and Shea Brown, Ryan Carrier, Merve Hickok, and Adam Leon Smith, *Bias Mitigation in Data Sets* at https://osf.io/preprints/socarxiv/z8qrb/.

[33] *Cf.* San Francisco City-wide IT focused –Disaster Preparedness, Response, Recovery, and Resilience Policy at https://sf.gov/resource/2021/disaster-preparedness-response-recovery-and-resiliency-policy-dpr3.

h. Require periodic updates to the Data Security Policy to ensure alignment with all applicable laws, regulations, and city/county objectives and plans.

3. Data Handling Systems.

All Data or data systems (hardware or software)used by the city or county, its representatives, and Applicable Third Parties, or interconnected to the Jurisdiction's network(henceforth referred to as a **"Data Handling System"**) shall provide mechanisms for compliance with the Jurisdiction's Data Security Policy. Such mechanisms should include, without limitation, the following:

a. All Data Handling Systems shall be subject to a security assessment and tested for vulnerability to unauthorized access or use prior to deployment.[34] These scans should be done on regular schedule as determined by the Chief Data Officer. If a Data Handling System employs any means of credit card transactions or interfaces with third party systems that employ such transactions, such Data Handling System shall comply with the provisions of industry standards such as the Criminal Justice Information Standard (CJIS) or the Payment Card Industry (PCI) Data Security Standard.

b. The city/county shall take additional precautions with respect to all Internet-accessible Data Handling Systems to safeguard against unauthorized information access or manipulation by outside actors. The Chief Technology Officer (or other appropriate leader of security and/or Information Technology on a city-wide basis) shall from time to time promulgate a series of tests using up-to-date federal standards for information assurance to ascertain the security of all Data Handling Systems against:

i. Unauthorized access to Data sources to access, alter, or erase Data.
ii. Malicious use of any internet technology designed to deceive or give misinformation to any users.
iii. Potential malware, malicious code, or hacking with the intent of compromising system integrity.
iv. Re-Identification of previously anonymous or De-Identified PII.[35]
v. Any other foreseeable risks that utilize flaws in the design of web applications or the implementation of the system to gain unauthorized access or hinder legitimate use of the system.

c. All Data Handling Systems shall utilize design standards for encryption of Sensitive Data and implement or mandate standards on all relevant components of such systems.

[34] *Id.*

[35] *Cf.* San Francisco's DataSF Open Data Release Toolkit at https://datasf.org/resources/open-data-release-toolkit/.

4. Compliance.

A compliance approach is necessary by supporting a structured team or implementing a standard process. Working with IT department teams to ensure that those requirements are implemented, and documentation is maintained is critical. This is a significant amount of work. If capacity is restricted, consider whether this is internal or external compliance (i.e., holding vendors accountable to requirements and audit checks).

The Jurisdiction's Data Security Policy and Data Handling Systems shall comply with all applicable laws, regulations and the Jurisdictions policies and practices. The city/county shall comply fully with applicable Public Disclosure Laws.[36] Legal notices and copyrights shall be included for disclosure purposes.[37]

5. Security Audits.

The city/county should conduct a periodic **"Security Audit"** at such intervals as are determined by the Controlling Authority and under the supervision of a recognized independent audit authority approved by the Controlling Authority. The primary functions of the Security Audit are to evaluate all Data Handling Systems and other mechanisms in place to ensure compliance with the Data Security Policy, protect information assets, and properly dispense information to authorized parties. Security Audits shall include evaluation of each pertinent system's internal design. Such evaluation must include, but is not limited to, efficiency and security protocols, development processes, and governance or oversight. Installing controls is necessary but not sufficient to provide adequate security. Security Audits must include a report on the implementation of this Policy. The auditor must consider whether the controls are installed as intended, if they are effective if any breach in security has occurred and, if so, what actions can be taken to prevent future breaches. These inquiries must be answered by independent and unbiased observers employed by the auditor performing the task of information systems auditing. The following principles and actions should be among those included in each Security Audit:

a. *Ensure Timeliness* through continuous inspection regarding potential susceptibility to known weaknesses.

b. *Provide Financial Context* through transparency of private or commercial development and funding for clarification.

c. *Facilitate Scientific Referencing of Learning Perspectives* by noting vulnerabilities and innovative opportunities.

d. *Foster Literature-Inclusion* by compiling a list of references in each audit report.

e. *Maintain Relevant User Manuals & Documentation* by checking and updating manuals and technical documentations during the audit.

[36] From City of Seattle Web Presentation and Accessibility Standards Version 3.0, October 2, 2012.

[37] *Id.*

f. *Identify References to Innovations* by testing with high priority applications that allow both messaging to offline and online contacts, such as chat and email.

g. Include, without limitation, the **"Web Presence Audit"** and **"Network and Communications Systems Audit"** components described in the following two subsections of this Section 3.B.

6. Web Presence Audits.

The extension of the Jurisdiction's presence beyond its internally controlled Data Handling Systems, network, and management domain (e.g., the adoption of social media by the enterprise along with the proliferation of cloud-based tools such as social media management systems) requires the city/county to incorporate Web Presence Audits into the Security Audit. The purposes of such Web Presence Audits are to ensure that the Jurisdiction and Applicable Third Parties are taking the necessary steps to:

- Prevent the use of unauthorized tools.
- Minimize damage to individual or entity reputation.
- Maintain regulatory compliance.
- Prevent information leakage.
- Minimize risks of harm from insufficient social media governance.
- Mitigate risks of harm from unanticipated or unintended consequences.

7. Network and Communications Systems Audits.[38]

The city/county should audit its network, including all interfaces and interconnections with third party networks and infrastructure, and its communications systems, whether controlled internally or purchased as a service, for compliance with the Jurisdiction's Data Security Policy. The "Network and Communications Systems Audit" should ensure that the Jurisdiction's network and communication systems:

- Adhere to stated policies adopted by the Jurisdiction.
- Maintain regulatory compliance.
- Follow policies designed to minimize the risk of hacking or phreaking.
- Prevent information leakage.
- Mitigate risks of harm from unanticipated or unintended consequences.

[38] *See* Michael Juergens, Social Media Risks Create an Expanded Role for Internal Audit, The Wall Street Journal, August 6, 2013 available at https://deloitte.wsj.com/articles/social-media-risks-create-an-expanded-role-for-internal-audit-1377532961 for discussion of this and other areas of precaution listed immediately above. A Jurisdiction may want to consider expressly adopting specific standards for these types of audits and cross-reference or attaching them as appendices to their Data Handling Policy. Several potentially relevant standards exist—for example see: Cybersecurity Framework published by the National Institute of Standards and Technology (NIST) at https://www.nist.gov/cyberframework; ISO 27001 at https://www.iso.org/standard/27001 (Information security management systems) and ISO 27002 at https://www.iso.org/standard/75652.html (Information security, cybersecurity, and privacy protection- Information security controls); and the GDPR. See also NYC Guidelines for the Internet of things at https://iot.cityofnewyork.us/data-management/ and https://iot.cityofnewyork.us/security/; San Francisco Citywide Cybersecurity Policy at https://sfcoit.org/cybersecurity.

For sample approaches to Data Security Policies, Data Handling Systems, cybersecurity, and related policies and practice tools, see the resources linked in the Data Management and Cybersecurity sections of the Resources Library.

C. Special Provisions for Open Data Programs

With respect to all of its Open Data Programs, it is recommended that the Jurisdiction:[39]

1. Make Data it collects discoverable and accessible to the public only through Data platforms that adhere to its adopted Data Governance principles and comply with its policies on Data quality and Data Integrity and its Data Security Policy.
2. Assess the Datasets to publish as Open Data, in accordance with standards and procedures established from time-to-time by a Data Governance Oversight Committee of the type described in Section 5 of this Guide), to identify risks of harm to personal privacy or personal safety and take steps to mitigate such risks.
3. Document the process for reviewing new Open Data requests, including who approves or denies the request and the rationale for the decision, and make the request, decision, and rationale available to the public.
4. Perform an annual risk assessment of the Open Data Program and the content available to the public pursuant thereto and present such report to the Data Governance Oversight Committee for its review, comments, and recommendations as to efficacy and risk mitigation strategies.
5. Provide a public process to allow individuals to review and contest Data that concerns their own individual personal information, whether or not such information is PII.
6. Provide to the Data Governance Oversight Committee an annual "Open Data Program Plan" and annually report on the assessment of progress towards achievement of the goals described in the Open Data Program Plan for the previous year.
7. Include in its Open Data portal and any similar Jurisdiction-maintained mechanism for publishing Open Data appropriate Limitation of Liability Provisions.[40]
8. To the extent prudent the Jurisdiction should:
   a. Publish high quality, public Data with documentation online.
   b. Ensure publishable Data is in the public domain and can be easily retrieved.
   c. Minimize limitations on disclosure of public information while safeguarding Sensitive Data.
   d. Encourage innovative uses of publishable data by agencies, the public, and other partners.

[39] Some of the following recommendations in this Subsection 3.C are based on or inspired by D.C. Data Policy at https://opendata.dc.gov/pages/data-policy. For other samples of Open Data Policies see the Open Data Policies section of the Resources Library.

[40] *See, e.g.,* D.C. Data Policy at X and XI.; City of Charlotte "Terms of Use" at https://charlotte.maps.arcgis.com/home/item.html?id=7c88b8633b034ddcbbd6badb1b7076fe; and City of Chicago Privacy Policy at https://docs.google.com/document/d/1hnmsJDkI4YmO8Pzk2yljFouwCFbdfbIfSn65Re074HU/edit.

SECTION 4: DATA USE RIGHTS AND DATA SHARING AGREEMENTS

A. Section Notes

Purposes. Cities and counties regularly engage in "data sharing" in many ways, including through Open Data Programs that make selected types of Data publicly accessible; in agreements with vendors, research organizations, or other for-profit or non-profit organizations of various types; in arrangements with other cities or counties, or with state or federal law enforcement or other agencies; and "internally" where two or more city or county departments or agencies identify data sharing requirements, needs, or potential benefits.

Prominent Challenges Addressed. The initial working group that led to the MetroLab Data Governance Task Force identified several scenarios, challenges and considerations regarding "Data Use Rights" and "Data Sharing Agreements," including:

- Negotiating policies and strategies with private companies—and building data governance terms and conditions into "Requests for Proposals" (RFPs) for technology procurements (e.g., software procurements).
- Determining who "owns" Data and what permitted or prohibited uses the Data owner and other parties may or should have.
- Exploring "opt-in" versus "opt-out" approaches to constituent consent to collection and use of their data.
- Dealing with vendor "opacity."
- Addressing special considerations with "hidden data" (e.g., metadata).
- Promoting inter-departmental Data sharing and opportunities from "overlays."
- Considering special arrangements when the Jurisdiction shares data with research organizations.
- How to approach formalization of arrangements with Data intermediaries.
- The importance of a team approach to Data Sharing Agreements in which Jurisdiction Legal Counsel and Information Technology personnel are among the team members.
- Special considerations regarding Open Data Programs.
- Special considerations with law enforcement Data
- Monitoring performance and compliance on Data sharing and permitted vs prohibited uses and remedies for related breaches of contract.

Special considerations regarding residents' rights regarding their Data acquired by a Jurisdiction are addressed in the Data Governance Principles in Section 2 of this Guide, and Data sharing through Open Data Programs is addressed in Section 3.C. Both a Jurisdiction's "Internal Data Sharing" (e.g., among Jurisdiction departments) and Data sharing with other governments are addressed in Section 5.B. This Section 4 focuses on Data sharing provisions included in documents for technology procurements from vendors (e.g., in RFPs) and negotiated Data sharing agreements with other non-governmental "external" parties, such as parties whose activities are subject to regulation by the Jurisdiction or organizations involved in research that might help inform Jurisdiction policies and practices or otherwise promote public good.

For a list of several sources providing background, and sample policies and practice tools associated with the issues addressed in this Section 4, see the Data Sharing Agreements and Additional Background Readings sections of the Resources Library.

B. Data Sharing Challenges/Common Considerations and Principles

1. Context and Threshold Guiding Principles.

With the volume, velocity, and variety of data expanding exponentially, Jurisdictions are increasingly employing Data sharing to innovate, fill knowledge gaps, and facilitate other parties' public good initiatives. For the purposes of this Guide, Data sharing, and acceptable use considerations are focused on Data the Jurisdiction (i) collects directly, (ii) receives through an agreement with a Data Intermediary or other Applicable Third Party engaged to collect the Data for the Jurisdiction, or (iii) has obtained from an Applicable Third Party and has permission to share.

The key to effective and appropriate Data sharing is for all impacted parties to have a common understanding of what Data will be shared, why Data sharing is warranted, the intended outcomes of the Data sharing, permitted and non-permitted uses of the Data, the Data management approach to be employed, and the roles and responsibilities of each party. The parties involved, and associated guiding principles, include:

- Data Owners: the onus is on the Data owners to specify the allowed uses and expected handling as well as to manage communications with other impacted parties.
- Data Recipients: Data recipients need a clear use case for the requested Data, robust processes to ensure that Data management expectations are met, and the ability to demonstrate appropriate use of the Data.
- Data Subjects: in the event the Data contains information about people, those persons should be notified prior to such Data sharing and should also be able to learn the outcomes of that Data sharing.

In line with Section 2, those parties and guiding principles should be considered and intentionally addressed when negotiating Data Sharing Agreements and Data Use Rights. Included below are a few additional comments related to principles and practices around ethical Data use and risk management.

2. Ethical Data Use and Risk Management.

Ethical Data use means using the Data to improve lives without introducing greater risk to those lives. While ethical Data use can be relatively straightforward for the Jurisdiction when collecting information in order to provide a service, the considerations are different when such administrative Data will be put to different uses through Data sharing. To determine if the Data sharing will result in continued ethical Data use, the following questions should be among those asked:

- Was the Data collected for a purpose that is similar to how it will be re-used? Dissimilar purposes may mean the Data will not inform the new use case.
- Is the Data quality suitable for the re-use purpose? Responses needed to fulfill a service request may be less rigorous than those sought to inform, e.g., trend analysis.

- Do the Data sharing use cases align with the Jurisdiction's priorities? Distinguish Data sharing that serves the public good from those with private financial or other purpose and ensure you have a public message around the Data sharing that aligns with your Jurisdiction's priorities.
- Does the data satisfactorily represent the Jurisdiction's community? Survey Data for which responses were received from predominantly one or two segments of the Jurisdiction's community may not be suitable for determining community perspectives as a whole.
- Does the Data sharing use case further an equitable community? Apply due diligence in understanding communities that benefit or may be excluded.

Risk appetite varies among Jurisdictions, with some being highly risk averse and others willing to accept some risk for potentially greater community rewards. Data sharing has a risk management component that needs to be aligned with the Jurisdiction's tolerance for risk. One consistent output of all Data sharing should be public communications - what Data sharing is occurring, why, and to what benefit? When managing risk, consider how the Data sharing message will be perceived by constituents and the Jurisdiction's leadership.

C. Data Sharing Provisions in Procurements

This subsection addresses provisions pertaining to Data sharing in the context of a Jurisdiction's procurements of technology from vendors of three types:

- **"Primary Vendors"** offering broad services to the jurisdiction including substantive Data Handling to support the services (generally persons and entities that deal in large quantities and diverse types of Data and/or are providing major Data Platforms or Data Platforms support to the Jurisdiction). Examples range from cloud-base administrative systems such as financial or permitting software to GIS, data warehouse, or data management platforms.

- **"Secondary Vendors"** offering services in specific data analytics or other targeted Data services (generally persons and entities that deal with Datasets more limited in nature than Primary Vendors). Examples include consulting firms engaged to perform analysis within a specific policy area and [not sure what else

- **"Miscellaneous Vendors"** that do not fit in with the previous two categories, but are engaged to provide goods and services, or are otherwise entering into agreements with the jurisdiction, in circumstances that are likely to produce significant Data that could be productively used by the Jurisdiction.

The Jurisdiction's procurement processes for engagements that directly or indirectly involve any aspect of Data Handling ("Data Handling Procurements") should follow the same principles, policies, and guidelines that apply to Data management within the organization. Accordingly, Data Handling Procurements, and related requests for proposals ("RFPs"), requests for information ("RFIs"), and requests for quotes ("RFQs") should reflect the following principles and practices:

a. The Jurisdiction shall recognize that the products and services it buys have inherent social, human, health, environmental and economic impacts, and that the Jurisdiction should accordingly make procurement decisions that embody, promote, and encourage a commitment to the community it serves.

b. Procurement officials and associated Jurisdiction employees shall apply due diligence in seeking to prevent or mitigate harm or inequity resulting from Data Handling.

c. To the extent deemed applicable by the Controlling Authority in the particular request regarding a Data Handling Procurement, require that respondents communicate how they will adhere to the Data Governance Principles adopted by the Jurisdiction and the additional guiding principles specific to Data use and Data sharing set forth in Subsection 3.B above.

In addition, the following specific measures and questions drawn from three sources shared by Task Force members might be considered for inclusion in RFPs, RFIs, and RFQs, as applicable:

From City of Asheville, NC *Technology Procurement Governance Checklist*:

Asheville uses a checklist to evaluate whether a vendor's product meets the City's data, security, accessibility, and other standards and makes the checklist available to vendors. See the "Questions" and "Why is it Important?" explanations associated with each of the twenty-one following named "Items" addressed in Asheville's checklist:[41]

- Data Ownership & Rights
- Data Privacy
- Confidentiality
- Data Center Security (SaaS)
- PCI Compliance
- Exit strategy (avoid lock-in)
- Data Standards
- Accessibility
- Software Usability
- Open, Published APIs
- Financial Integration
- Other Data Integration Needs
- Public Record Law
- Data backup and disaster recovery
- Service Level Agreement
- On-Premise infrastructure requirements
- Access needed to on-premise infrastructure to our network
- Webforms
- Equity and Digital Inclusion
- Portfolio Alignment or Duplication
- Administrative Rights

[41] Quoted *verbatim* from City of Asheville, NC Technology Procurement Governance Checklist at https://docs.google.com/spreadsheets/d/e/2PACX-1vTNefGUaZ7E1eLfGcaukzdbqYKpTPyl6G9DvNqOyM9kPA0dKr-zPmBU7syKIQeQodWiQvzq66HwvWHs/pubhtml?gid=0&single=true.

From *Platform Urbanism Data Sharing Policy Guidelines*:

While the context of Platform Urbanism Data Sharing Policy Guidelines[42] is regulation of sharing economy platforms, the following seven named guidelines it sets out can also have relevance to a Jurisdiction's procurements as well:

1. Justify and focus data sharing requirements by defining government objectives and documenting use cases.
2. Commit to minimizing platform data collection to the least invasive information needed to meet program objectives.
3. Specify fields and frequencies to cater data granularity appropriately.
4. Require machine-readable, open formats and standards, and consider appropriate data transfer approaches.
5. Commit to program transparency, public oversight, and ongoing feedback.
6. Establish organizational structure for [data sharing requirements] implementation, including roles, responsibilities, and enforcement mechanisms.
7. Classify, protect, and permission Sensitive Data.

Sources underlying those seven guidelines and "Example Policy Language" are available in the PUDS Policy Guidelines site.[43]

Some Additional Recommendations for Data Sharing in the Procurements Context:

Also consider incorporating each of the following in planning and setting the proposed terms of a technology procurement that will involve Data Handling: [44]

- Involve the Jurisdiction's Legal Counsel throughout the process of fashioning Data sharing and related provisions in the applicable procurement documents. Include in their review and analysis responsibilities due diligence in pursuit of the goal that none of the collection, storage use and/or disseminated of the applicable Data will conflict with applicable law or with guiding principles adopted by the Jurisdiction regarding Data sharing. Require Legal Counsel to engage with IT Staff in those due diligence efforts.
- Clearly define what constitutes a Data breach and what the responsibilities of the vendor are in relation to lessening the risks of a data breach and in relation to potential liability as a consequence of a data breach.

[42] Except as otherwise indicated in brackets, the following seven points are quoted verbatim from Platform Urbanism Data Sharing Policy Guidelines ("PUDS Policy Guidelines") available at https://sites.google.com/view/datasharingpolicyhub/policy-guidelines#h.895fmaqceyxj.

[43] *Id.* In addition, we note that we understand that those principles were inspired by the work of Beatriz Botero Arcila—see, e.g., Beatriz Botero Arcila, *Sharing Data in the Sharing Economy: Policy Recommendations for Local Governments*. 9 Indiana J. Law and Social Equity 1 (2021) available at https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1119&context=ijlse; and Beatriz Botero Arcila *The Case for Local Data Sharing Ordinances,* 30 Wm. & Mary Bill Rts. 1015 (2022) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3817894.

[44] Based largely on appendices in the 2020 Draft Data Handling Policy (on file with the Guide editors).

- Address how the Jurisdiction and the vendor will implement their performance obligations after a contract is signed, including, as applicable, reporting and monitoring obligations.[45]

D. Data Sharing Agreements with External Parties in Other Contexts

This subsection addresses Data Sharing Agreements which do not involve any payment by the Jurisdiction to an "external" party of the either of the following types:

- "**Private or Non-Profit Sector Parties**" that (i) are subject to regulation by the Jurisdiction or (ii) provide data to the Jurisdiction and/or receive data from the Jurisdiction for the purpose of jointly providing a new or improved service to the community for the public good.
- **"Academic Parties**" that generate data on behalf of the jurisdiction and/or process jurisdiction data and typically resourced by grants and other public funding.

Regardless of which of those types of parties are involved, the overarching considerations are common to both, and essentially mirror the considerations addressed in Subsection 4.C above regarding Data sharing provisions in technology procurement processes and documents—*and* implicate the same issues to address and due diligence and other recommendations made in that subsection.

In general, the fact that context does not involve a financial payment by the Jurisdiction to the one or more other parties in the Data sharing arrangement does not render any of those recommendations irrelevant. Indeed, some Task Force members expressed the opinion that special types of Data Sharing Agreements for arrangement with nonprofits or in other non-procurements settings are unnecessary. However, other Task Force members felt that there is value in having special forms/templates for non-procurement scenarios, as there can be some additional considerations to take into account in such situations. Such additional considerations might include, for example:

- Specialized licensing terms/use rights that take into account the nature of the collaborators (e.g., where they are educational institutions or nonprofit entities serving public benefit roles.
- In research collaborations, special attention to Institutional Review Board compliance or similar requirements to which one or more of the participating organizations are subject, and to the fact that some research collaborations may span long periods of time.
- Special provisions for parties serving as Data Intermediaries may be in order.
- Crafting measures of damage for breach of obligations that are not informed by contract payments.

For references to some resources containing sample Memorandum of Understanding (MOU) approaches to multi-party data collaborations among government agencies and nonprofits on matters involving education, homelessness, housing, and other issues, see the Data Sharing Agreements section of the Resources Library.

[45] For an illustration of the importance of follow through on RFP language in negotiating Data and implementing contractual Data sharing agreements, see Megan Marini, Troy Simpson, and Priyanka Jain, *A Rhode Trip: Lessons for the Future of Mobility From the Little Roady Autonomous Microstransit Pilot* (2022) available at https://rosap.ntl.bts.gov/view/dot/64116 at Section 5.2 Vendor Procurement (discussing, among other things, data reporting requirements in an RFP that "were ultimately relaxed during contract negotiations").

SECTION 5: THE "OPERATIONALIZING HOW": OVERSIGHT, ORGANIZATION, INTER- DEPARTMENTAL PROCESSES, AND COMMUNITY ENGAGEMENT

A. Section Notes

Purposes. Data is an asset only if it is responsibly used to enhance the efficiency of cities and counties and improve residents' quality of life. While protecting data from outside threats is a major concern in a Jurisdiction's Data Governance, just as important is standardizing internal departmental procedures to safeguard data throughout its lifecycle. Such procedures should ensure data integrity, interoperability, accessibility, and security from the prying eyes of unauthorized individuals–even unauthorized individuals who work for a Jurisdiction department or agency.

Prominent Challenges Addressed. The initial working group that led to the MetroLab Data Governance Task Force identified several categories of challenges and considerations in "operationalizing" city or county Data Governance, including:

- Limited resources and the consequent need to leverage existing resources.
- "Change management" and trust issues when implementing Data Handling system changes (and connections to enterprise-wide systems).
- A need to consider centralized oversight of data sharing requests and tech procurements.
- Having qualified legal counsel regularly engaged in shaping and maintaining Data Governance policies and practices.
- A need for better data mapping and better coordination of efforts among stakeholders.
- The importance of regularly evaluating how the Jurisdiction's Data Governance policies and practices are performing.
- The degree of thoughtful design needed to establish Mechanisms for inclusive, diverse, timely and meaningful community input on Data Governance policies and practices and reporting back to community on how such input was taken into account—including establishing effective means of collaborating with community members/community representatives on Data Governance matters in an accessible manner—e.g., translating tech jargon into functional terms with illustrations of the what, how, and why of specific data collection and use proposals.

Some Threshold Considerations on Operationalizing Data Governance:

- Data Life Cycle. To understand the "how" of operationalization, we must first consider the "what" of operationalization. A holistic approach to Data Handling requires looking at it from end-to-end. Therefore, as background on the operations governing structure please see the Data Life Cycle Graphic which offers an overview of what the data lifecycle looks like for a city or county (small or large) and cross-references what this Guide has already addressed in the previous sections.

- Consulting Units vs. Central Data Authority. "Data teams" often start off as consulting units where they are primarily providing consulting and data support to the different departments. However, as the data team matures it should move away from a consulting model to a central data authority model responsible for setting standards for data handling throughout its lifecycle. This Section 5 offers detailed recommendations for such a central data authority approach.

- Right-Sizing. As noted in the Preamble to this Guide, cities and counties differ in resources and levels of maturity in their Data Handling systems and processes. At least in the short term, the recommendations in this Section 5 may be more challenging to implement in some Jurisdictions than in others. Some "right-sizing" may be required, which might include additional training of some existing personnel to perform key functions described below, as opposed to creating new full-time positions.

- Creating and Maintaining a Data Inventory/Catalog. Among other matters that involve significant feasibility considerations is the question of the extent to which a city or county might endeavor to compile, and curate on a continuous basis, a comprehensive inventory of the Data it handles (a "**Data Catalog**").[46] Data Governance logically calls for a Jurisdiction to identify what Data it needs to govern. However, maintaining a Data Catalog that lists all Data/Datasets being collected or stored by or on behalf of a city or county, and of the processes by which such Data may be made available to various types of parties, is a very large and daunting task—even for Jurisdictions with substantial resources and mature Data Handling systems and processes. Accordingly, "right-sizing" of a Data Catalog effort may entail prioritization of types of Data and/or more of a "where and how" to look, who should look (and what training they need in that regard), and protocols for looking for specific categories or types of Data rather than an attempt to be assemble and curate a "comprehensive" inventory. It is recommended that at least that latter approach be considered.

B. Roles and Responsibilities of Jurisdiction's Primary Data Governance Personnel

It is recommended that a city or county have a **"Data Governance System"** to provide consistently applied processes, with checks and balances, for managing all aspects of Data Handling by the Jurisdiction and Applicable Third Parties. The Jurisdiction should adopt, implement, and maintain mechanisms for oversight of its Data Handling System to ensure compliance with its Data Governance Principles and Data Security Policy, and consider including in its Data Governance System, in addition to any other components it deems appropriate, the interdependent roles, responsibilities and processes set forth in the following provisions of this Section 5.

1. Chief Data Officer. The Controlling Authority should designate a **Chief Data Officer** to oversee all significant aspects of Data Handling and compliance with this Policy on a day-to-day basis, and

[46] For some examples of Data inventory and Data log approaches, see Data Policy Section V (Enterprises Dataset Inventory, Classification & Prioritization), Section VII (Data Catalogs—addressing both Open Data Catalog and Internal Data Catalog) and "Enterprise Dataset Inventory" and "Other Data Catalogs" parts of D.C. Data Policy at https://opendata.dc.gov/pages/edi-overview; and San Francisco Data Management Policy at 1.0 (Database and Data Inventories) at https://sf.gov/sites/default/files/2021-05/Data%20Policy_APPROVED%201.17.2019_0.pdf and San Francisco "Dataset inventory" at https://data.sfgov.org/City-Management-and-Ethics/Dataset-inventory/y8fp-fbf5.

also appoint an Open Data Programs Manager to oversee the implementation and management of the Jurisdiction's Open Data Programs and related policies and infrastructure. In some municipalities, the duties and functions of the Chief Data Officer may be shared with a "**Chief Information Officer**" or other Jurisdiction employee responsible for overseeing data security and data integrity measures, or the same person may hold both positions. The roles and responsibilities of the Chief Data Officer should include, in addition to such other matters as the Controlling Authority may designate:[47]

a. Managing the safeguarding of the Jurisdiction's Sensitive Data.

b. Ensuring that the data and network security provisions described in Section 3, including, without limitation, the tests and audits described therein, are implemented.

c. Help Jurisdiction departments/agencies make better use of available Data.

d. Connect citizens with Jurisdiction Data to promote public benefits.

e. Maintaining and keeping up-to-date systems designed to ensure compliance with Privacy Laws, Public Disclosure Laws, and other applicable laws and regularly engaging with Jurisdiction **Legal Counsel** and **Information Technology (IT) Staff** in those efforts—including on matters of encryption, cybersecurity, and evolving best practices in view of the evolution of pertinent technologies.

f. Designating and training a **Unit Data Steward** for each Jurisdiction department and agency, with input from each such unit on such designation and training.

g. Coordinating with, as applicable, the "Chief Innovation Officer," "Chief Information Officer", and/or "Chief Technology Officer (as applicable with respect to matters relating to data security), the **Open Data Programs Manager**, and all Unit Data Stewards and creating systems and structures that promote teamwork and feedback loops to help reap the benefits of Data gathering and analytics in a manner consistent with the Jurisdiction's Data Governance Principles, and in accordance with consistently applied quality assurance, accountability, and ethical standards.[48] Among other things, this coordination function should include attention to intra and inter-departmental data sharing (**"Internal Data Sharing"**). Data sharing with external parties such as vendors and educational institutions is addressed in Section 4 above. However, as part of data governance, Internal Data Sharing can be equally challenging. External data sharing standards should be applicable to internal data sharing as well especially if the

[47] Some elements of the following are based on the description of suggested roles for a government Chief Data Officer set forth on pages 3 and 4 (in Introduction by Sonal Shai and William D. Eggers) of The Chief Data Officer in Government: A CDO Playbook (Deloitte Insights – Beeck Center: Social Impact + Innovation at Georgetown University, 2018) available at https://www2.deloitte.com/content/dam/insights/us/articles/4577_CDO-playbook_DATA-act/CDO%20playbook.pdf.

[48] *Cf.* San Francisco Data Management Policy at https://sf.gov/resource/2021/data-management-policy and Citywide Data Classification Standard at https://sf.gov/resource/2021/data-classification-standard (read together defining and addressing coordination among people in the positions of "Chief Data Officer", "City Chief Information Officer", Cybersecurity Officers and Liaisons", "Privacy Officer", "Data Coordinators", "Data Stewards", "Data Custodians", and "Data Users").

department is independent or quasi-independent such as the police department. Diligence regarding Internal Data Sharing before it occurs should include:

i. Reaching agreement on purposes for which the requested data can be used and making sure they are consistent with the Jurisdiction's Data Governance Principles.
ii. Ensuring that the requested Data use clearly demonstrates the benefits and value of data sharing.
iii. Committing to a retention duration and ensuring that Data is deleted post expiration of the retention period.
iv. Agreeing on the degree of access the department personnel will have to the data.
v. Determining whether there are special considerations to address when the Internal Data Sharing may involve particular types of governmental operations—such as city or county law enforcement, relationships with state or federal law enforcement (e.g., taxing or immigration law authorities), or public schools.

Examples of approaches to Internal Data Sharing appear in several resources cited in the Resources Library.[49]

2. ***Open Data Programs Manager.*** The Open Data Programs Manager – who in some Jurisdictions might be the same individual as the Chief Data Officer – would manage the Jurisdiction's Open Data Program, and in performing that function:

a. Coordinate the publication of public data from Jurisdiction departments, agencies, and commissions on the Jurisdiction's Open Data portal;[50] and

b. Be responsible for completion of all actions and reports required with respect to the Jurisdictions Open Data Programs described in Section 3.C of this Guide.

3. ***Unit Data Stewards.*** The Chief Data Officer will designate a Unit Data Steward for each department and agency (each a "Unit"), in each case in consultation with the Unit. A Unit Data Steward must be a Jurisdiction employee with other significant duties within the applicable Unit or significant prior experience with the particular functions and practices of that Unit. The responsibilities of a Unit Data Steward include:

[49] *See, e.g.,* "Data Management Strategy Overview" section of City of Dallas Data Management Strategy 2019-2022 at https://dallascityhall.com/departments/ciservices/DCH%20Documents/Data-Management-Strategy.pdf#search=data%20privacy; and D.C. Data Policy at Section VIII (Streamlined Processes for Interagency Data Sharing) at https://opendata.dc.gov/pages/data-policy.

[50] *Cf.* Section 2-2134 of the KCMO Open Data Policy at https://library.municode.com/mo/kansas_city/codes/code_of_ordinances?nodeId=PTIICOOR_CH2AD_ARTXVIOPDAPO.

a. Developing and maintaining a concrete understanding of:

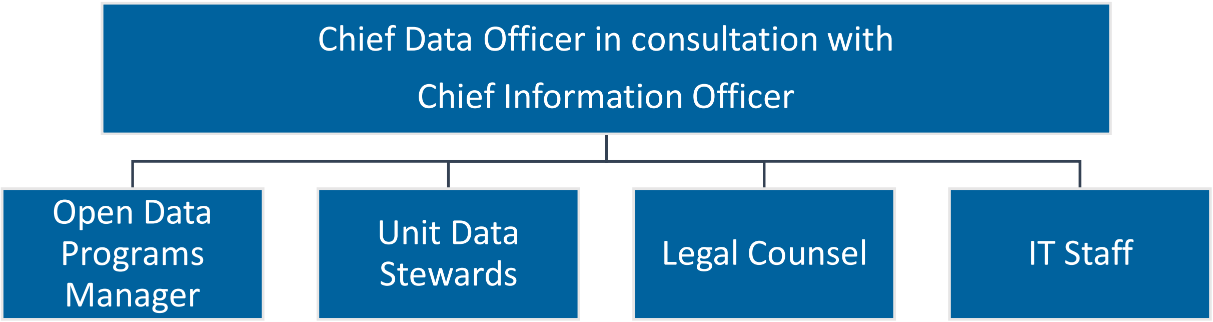
(i) the inner workings and outer relationships of the Unit regarding Data Handling;
(ii) the ability to recognize and classify Sensitive Data collected or generated by the Unit; and
(iii) familiarity with the requirements of Privacy Laws and Public Disclosure Laws that may apply to the Unit's Data Handling.

b. Updating the Chief Data Officer on new data availability, data issues, and system changes.

c. Making recommendations to the Open Data Programs Manager as to what Data collected or generated by the Unit the City should make available to the public as Open Data.

d. Offering suggestions to other personnel in the Unit as to ways responsible and unbiased analysis of Data available to the Unit can improve the efficiency, quality, and positive impact of the work of the Unit.

A general overview of the foregoing organizational structure follows (Source: Authors):


Chief Data Officer in consultation with
Chief Information Officer
Open Data Programs Manager
Unit Data Stewards
Legal Counsel
IT Staff

For other examples of Data Governance organizational structures adopted by Jurisdictions, see resources listed in the Data Management, Data Governance Policy, and Operationalization sections of the [Resources Library](). [51]

[51] For example, see City of Dallas, TX Data Governance Structure graphic in Figure DGS 1 at https://dallascityhall.com/departments/ciservices/DCH%20Documents/Data-Management-Strategy.pdf#search=data%20privacy.

C. Comprehensive Oversight Model.

This subsection provides an example of a comprehensive model for Data Governance oversight. It includes multiple layers and groups of staff and external stakeholders, including community members. Elements of these groups could be implemented in different ways depending on the Jurisdiction's resources and organizational capacity. Subsection D. below provides additional recommendation on how to involve the community in the design, maintenance, accountability, and oversight of the Jurisdiction's Data Governance System.

1. Data Governance Oversight Committee.

The Jurisdiction should create a "Data Governance Oversight Committee" comprised of the Chief Data Officer, the Chief Information Officer, and the Open Data Programs Manager, Legal Counsel (e.g., a designated City Attorney), and the Community Advisory Body (CAB) "Convener" described in D. below, and have the following authority, responsibilities, and general operating rules:

a. Act as an "executive committee," chaired by the Chief Data Officer, in overseeing adherence to all significant elements of the Jurisdiction's Data Governance mechanisms, including, without limitation, making recommendations on matters that allow for optional means of compliance or expressly contemplate discretionary actions.

b. Recommend (i) modifications to the Jurisdiction's Data Governance System when the Committee deems such modifications necessary to better adhere to the Jurisdiction's Data Governance Principles or to respond to developments in technology or other circumstances that necessitate such modifications to facilitate such adherence, and (ii) steps to clearly communicate such modifications to Jurisdiction personnel (including unit-level Data Stewards), to other participants in the Data Governance System, and to the public.

c. Review all Jurisdiction audit reports relating to Data Handling and make any recommendations to the Chief Data Officer deemed appropriate based on such reports.

d. Periodically review the Jurisdiction's training programs relating to Data Handling and provide recommendations to the Chief Data Officer regarding such programs.

e. Provide advisory input to the Chief Data Officer on other matters or decisions regarding Data Handling on which it is asked to provide such input by the Chief Data Officer or by the Community Advisory Board (CAB).

f. In its work on significant Data Handling matters actively engage the CAB to gather informed and timely community input and channel it to the Committee, and then deliver such community input, together with any observations or recommendations it makes based thereon to the Chief Data Officer.

g. Hold regular periodic meetings to facilitate performance of its functions and hold special meetings, whenever the Chief Data Officer or a majority of the Committee deems necessary or appropriate and develop other operational rules the Committee deems appropriate to perform its functions in a manner consistent with the Jurisdiction's Data Governance Principles.

2. Community Advisory Board (CAB).[52]

The Jurisdiction should create a "Community Advisor Board (CAB)" consisting of a "Convener," who shall be a non-voting *ex officio* member of such Board, and a reasonable number of regular Board members. The regular Board members should be or represent diverse community stakeholders. Accordingly, efforts should be made to include as regular Board members representatives of: neighborhood associations, educators from varied disciplines (including, among others, human sciences such as ethics, philosophy, psychology, and sociology), the business community, the technology community, and nonprofit organizations that promote public health and safety, workforce development, and equitable opportunities for well-being for vulnerable populations such as disabled, aging, and low-income residents.

Functions of the CAB:

a. The CAB's primary function is to provide the Data Governance Oversight Committee with informed, timely, and diverse community input and recommendations on Jurisdiction Data Handling matters and decisions (i) on which the Data Governance Oversight Committee requests such advisory input and (ii) that the CAB determines should be brought to the attention of the Data Governance Oversight Committee.[53] In performing its primary function, the CAB shall seek to (i) advance adherence to the Jurisdiction's Data Governance Principles, and (ii) develop systems and methods for gathering, memorializing, and reporting to the Data Governance Oversight Committee informed, timely and diverse community input and recommendations that are well designed and tailored for particular Data Handling matters and decisions it is addressing (i.e., not "one-size-fits-all").

b. The CAB should all also collaborate with the Community End User Testing Group described in subsection 5.D to facilitate diversity and timeliness in participation by community stakeholders in that Group's work.

[52] The following description of the Community Advisory Board is based on an amalgamation of study of various advisory or similar boards created in Chicago, Kansas City, MO, San Francisco, Seattle, and other cities, interviews or other discussions with individuals involved in such initiatives, and observations made by students, faculty, government personnel, and various collaborators in the Draft Data Handling Policy project through several semesters of the interdisciplinary UMKC Law, Technology, and Public Policy course described in the Preamble to this Guide. A regional approach to the CAB might be efficient and appropriate in some regions—i.e., one independent body that could help gather and channel informed and timely input from multiple community stakeholders to Data Governance decision makers or a city or county advisory board in any city or county in the region.

[53] *Cf.* Seattle Community Technology Board statement at https://www.seattle.gov/community-technology-advisory-board/what-we-do/committees ("Issues are referred by the Mayor and Councilmembers or come from community input.").

c. The CAB should have regular meetings, at appropriate intervals determined by the Jurisdiction, as well as special meetings when called by the Convener (with notice reasonable in the circumstances presented). The CAB shall fix its own operating rules and procedures in a manner appropriate for its above-described functions.

Designation and Functions of the Convener:

a. Subject to c. below, the Convener should be an individual designated by the Controlling Authority under such process and for such term of service as the Controlling Authority determines.[54]

b. Subject to c. below, the regular Board members should be individuals designated jointly by the Chief Data Officer and the Convener to serve for such term of service as is determined by the Controlling Authority.[55]

c. In no event should any person be appointed as Convener or a regular Board member if such individual is (i) an employee of the City; (ii) a contractor with the City; (iii) an owner, officer, employee, agent, or representative of a for-profit business engaging or seeking to engage in a contract or other commercial relationship with the City; or (iv) a spouse, parent, child, sibling (including those related by marriage) or significant other of, or any person who resides with, a person described in (i), (ii), or (iii).

d. The Convener should:

(i) Present an annual budget for the CAB to the Controlling Authority to secure resources needed for the CAB to operate.

(ii) Set the agenda for each CAB meeting, with input from the regular Board members.

(iii) Call special meetings of the CAB as and when needed.

(iv) Administer the conduct of all CAB meetings.

(v) Manage the process of having the Board prepare and deliver reports its input and recommendations to the Data Governance Oversight Committee.

(vi) Serve on the Data Governance Oversight Committee and, in that connection, monitor the extent to which the CAB's input to that Committee is taken into account in its work, and report to the regular CAB members on the disposition of its input and recommendations.

[54] The time commitment of the Convener would be substantial, and it is presumed compensation would be paid.

[55] A question to consider here is whether the Board members could/would be unpaid volunteers. As reflected in Subsection 5.D below it is recommended that a Jurisdiction strongly consider paying community members involved in its Data Governance System for their associated time.

(vii) Prepare and deliver to the CAB and the Data Governance Oversight Committee an annual report summarizing the activities and impact of the CAB for the reporting year.

3. Civic End User Testing Group (CEUTG).[56]

The practice of having a "Civic End User Testing Group" can serve important purposes that relate to Data Governance but also advance a Jurisdiction's public service objectives in the context of testing operations where "data" is not the primary focus. In essence, such a group can bring a diversity of community perspectives to bear in the co-design of improvements to Jurisdiction systems with which community members interact.

Under the direction of the Data Governance Oversight Committee, the Jurisdiction should create a Civic End User Testing Group ("CEUTG"). The CEUTG would provide feedback regarding the use and accessibility of the Jurisdiction's Open Data resources, websites, applications, and other citizen interfaces.

a. The CEUTG should be composed of community users possessing a variety of technological skill levels. The CEUTG will seek input from the Community Advisory Board (CAB) on inclusiveness and diversity of community users.

b. The Jurisdiction would solicit participation in user testing through its existing websites and applications or other means, with advisory input from the CAB, and in doing so may pose eligibility questions to ensure participants represent a variety of skill levels.

c. The Jurisdiction might incentivize participation in the CEUTG testing by providing testers with small monetary awards for completing applications and testing.[57]

d. The CEUTG would report feedback from its user testing activities directly and simultaneously to the Data Governance Oversight Committee and the CAB.

For other examples and practice tools regarding end-user testing as part of city or county Data Governance Systems, see resources listed in the Community Engagement and Resident Feedback section of the Resources Library.

[56] *Cf.* Chicago City Tech Collaborative Civic User Testing Group (CUTGroup) described at https://www.citytech.org/resident-engagement and KC Digital Drive, Code for KC, and Missouri Western University launch of Kansas City's first civic UX testing group at https://www.kcdigitaldrive.org/article/get-your-community-websites-apps-tested-by-kcs-first-civic-ux-group/. "CUTGroups" have been organized in several other cities as well—see, e.g. https://datadrivendetroit.org/blog/2018/03/23/cutgroup/ (Detroit); https://medium.com/@seattle.cutgroup/establishing-a-seattle-civic-user-testing-group-48ea6ef58b86 (Seattle).

[57] One of the ways the Chicago CUTGroup has engaged their community in its activities is by giving participating residents who test civic websites and apps gift cards. See https://irp-cdn.multiscreensite.com/9614ecbe/files/uploaded/TheCUTGroupBook.pdf at page 1.

D. Community Engagement Needs and Methods.

Community participation in a city's, or county's Data Governance is essential for Data to become a community asset. Oftentimes, Data-related policymaking can be opaque or unaccountable to those experiencing the greatest risks of Data harms. There are important opportunities for communities to contribute to the design of Data Governance policies and practices, help hold organizations accountable, and improve communications. Creating spaces for communities to meaningfully contribute requires resources, time, and relationship building. These investments will improve Data Governance impacts and outcomes. A Community Advisory Board (CAB) as described in Subsection 5.C above would obviously be one key element of community engagement—one that we recommend can and should play role in supporting it—but the need for community engagement extends well beyond the oversight function of that body.

1. Engagement Planning

It is recommended that a Jurisdiction begin with proactive planning for any interaction or request of a community member's time. Community members (and staff) have limited time and overlapping urgent priorities. Before designing an engagement, identify the goal and what can be provided to the participating community members in terms of how their input will be used and how the Jurisdiction will report back on the final impact of their participation. Depending on the identified goals of the community engagement, different forms of public participation may be necessary or useful:

- Inform
- Consult
- Involve
- Co-create/collaborate
- Defer to community ownership

The Jurisdiction might in this connection review *Facilitating Power's Spectrum of Community Engagement to Ownership*[58] or the International Association for Public Participation's *Spectrum of Public Participation*[59] for more details on different types of participation. Being explicit about the Jurisdiction's Data Governance goals and how they relate to the ways community members interact with the Jurisdiction allows communities to know what to expect and how they can participate.

Data Governance has many components. Information sharing events and materials may help prepare a variety of audiences to be able to sit at the same table for more collaborative engagements and involvement in the Jurisdiction's Data Governance practices. Design presentations or materials with accessible language and examples that connect to community member's daily lives or common interactions they have with the city or county. For example, community members are often required to

[58] At https://movementstrategy.org/wp-content/uploads/2021/08/The-Spectrum-of-Community-Engagement-to-Ownership.pdf.

[59] At https://cdn.ymaws.com/www.iap2.org/resource/resmgr/pillars/Spectrum_8.5x11_Print.pdf.

share personally identifiable information (PII) when paying a bill or perhaps share anonymous demographic information about themselves when accessing a new service. Understanding how that Data is managed, who has access to it, and a clear reason for how and why you will use that Data are outcomes of Data Governance that will benefit community members.

Data that the city or county is collecting or managing through its Data Governance System is often about and from communities. Community members are experts on their lived experiences. Knowledge and expertise of community members most susceptible to harm from Data are also required to disrupt existing harmful Data collection and analysis practices. By partnering with communities and leading with community driven needs, challenges, and strengths, the Jurisdiction may be able to prioritize where to focus Data Governance efforts if resources are limited. Here are several examples of Data Governance practices that would be served well by collaborative, co-design, or defer to styles of community engagement:

- Data collection best practices and trainings
- Demographic Data standards
- Communicating what, why, and how Data classifications are used
- Open Data priorities and how well open data is working for communities
- Data collection and Data use expectations for grants or contracts with community-based organizations
- Updating or maintaining relevancy of Data Governance practices to be most responsive to community data needs

If throughout the development and implementation of Data Governance community engagement, the types of approaches utilized all fall on the informing or consulting end of the engagement spectrum, trust and partnership with communities may not be improved. It may require more staff time and resources to design interactions on the involve, collaborate, and defer to end of the spectrum, but the potential to thereby increase trust is also much greater. Note that there may be other aspects of existing Data Governance structures and/or leadership preventing meaningful contribution from communities. Identifying such impediments is necessary to find solutions or to communicate these limitations directly with community members.

2. Accountability

As Data Governance policies and practices are adopted, communities can play several roles for accountability.

Section 5.C of this Guide details a comprehensive oversight model with a formalized Community Advisory Board and Civic End User Testing Group. This model requires that budgets available for the groups, stipends, and staff resources to adequately support the groups. Committee members in voluntary oversight or advisory bodies may quit if commitments are burdensome. To be effective, committee members need information and support.

If a group is an advisory body, there needs to be clarity on who is ultimately the decision maker and how these decisions are made. This supports understanding of how information provided by committee members is or is not used. If a group is an oversight body, they need access to information about how implementation is going, where challenges are arising, and authority to make sure commitments are met. For example, a 2019 City of Portland Audit found that "if a government body commits to public oversight, it must work to ensure that participation is meaningful because ineffective participation can jeopardize public trust and waste resources and time." [60]

Accountability with communities may also be achieved through implementing other types of engagements. Accessible information sharing and meaningful education opportunities to create awareness about adopted Data Governance Principles and Data Governance practices are first steps. If these are implemented along with a clear contact at the organization, a community member or community-based organization can raise a flag if they see a practice being violated by staff. This places the burden on civic engagement and advocacy to flag but could be a minimum starting point.

3. *Community Involvement and Partnership*

Community involvement and collaboration-style engagements can also be used for accountability touchpoints. This would require staff to prepare accessible report outs on implementation progress and what decision points communities can weigh in on to help assess the Jurisdiction's Data Governance. Active involvement of communities in the design of Data Governance policies and practices allows communities to be able to identify if and how community needs they know were shared are being incorporated or not.

One last model that could be incorporated into any of the above pieces is a community-government partnership model where community leaders are hired and paid as consultants.[61] For example, the City of Portland Smart City PDX has implemented several iterations of this model documenting lessons learned from each year. Qualifications for community leaders can come from a range of experience including volunteering, organizing, or work. Below are examples of how Smart City PDX defines community leader excerpted from the 2021 Request for Qualifications:[62]

> "As a Community Lead, you are eager to build inclusive technology and collaborative decision-making spaces through thoughtful partnerships between frontline communities and the Smart City PDX program. You are a connector - ready to think about how to link digital justice with the many priorities communities are already navigating. You are an organizer - ready to bring your community and their voices into the digital justice movement. Most of all, you are excited to work with a team of people who each have different skills, visions, and perspectives on what digital justice looks like."

[60] See https://www.portland.gov/sites/default/files/2021/report-web.pdf.

[61] See example in Portland, OR at https://www.smartcitypdx.com/news/an-opportunity-for-community-leaders.

[62] See https://static1.squarespace.com/static/5967c18bff7c50a0244ff42c/t/611adc797143ff4af062e56e/1629150329289/Community+Leads+Request+for+Qualifications+Due+Sept+7+2021+at+5pm.pdf.

In this model, community leaders become a part of the Jurisdiction's team to help design and implement new practices of centering community. These leaders have existing relationships with impacted communities. These positions help expand the team. They could be used to support a successful advisory committee body. Community leads can help design and implement engagement events that may bring new participants, beyond those who would attend events designed and led by staff alone. This same model could be achieved by contracts with community-based organizations to help build new relationships, expand involvement, and ultimately achieve data governance that serves your communities.

For other examples of collaboration-style community involvement in the design of Data Governance policies and practices see resources listed in the Community Engagement and Resident Feedback section of the Resources Library.

E. Liability Limitations, Governmental Immunity, and Cyber-Insurance

As indicated earlier in this Section 5, it is essential that a Jurisdiction's Legal Counsel be regularly and closely involved in its Data Governance System and related oversight mechanisms. A city or county attorney's roles should include, among other things, identifying potential risks of liability and recommending measures to help eliminate or mitigate the Jurisdiction's exposure to liability associated with its Data Handling.

1. Liability Limitation Measures.

The Jurisdiction, with advice from its Legal Counsel, should in its Data Handling activities adopt and adhere to appropriate terms of use, disclaimers, exclusion of warranties, and other limitation of liability statements or provisions, monitor the effectiveness of such provisions, and seek to modify them when deemed necessary or appropriate based on experiences, technological developments, or other circumstances. These types of provisions of course must take into account applicable laws and should seek to follow best practices. Readers are encouraged to review relevant sections in resources listed in the Data Management, Open Data Policies, and Data Governance Policies sections of the Resources Library.[63]

F. Governmental Immunity and Cyber-Insurance.

To the extent, if any, that the Jurisdiction's Legal Counsel determines that "Governmental Immunity" does or may not apply to any part(s) of the Jurisdiction's Data Handling endeavors, or that it is otherwise desirable, the Jurisdiction might consider purchasing appropriate cyber-insurance for coverage related to loss or damage resulting from a Data hack/breach or spillage of Data.[64] Issues

[63] See, e.g., examples cited in footnote 40 above.

[64] For general information regarding some of the issues that may be involved in this connection, see, e.g.: *Sovereign immunity in the age of continuous cyber warfare* at https://www.bricker.com/insights-resources/publications/sovereign-immunity-in-the-age-of-continuous-cyber-warfare (July 15, 2015);

relating to whether or not a city or county has “Governmental Immunity” against liability for damages caused by Data hacks or breaches are quite complex, and can vary among Jurisdictions by reason of differences in state laws and other circumstances. A Jurisdiction should have its Legal Counsel explore them as well as the terms and implications of obtaining cyber-insurance. *For additional background in this connection, see relevant readings listed in the Additional Background Readings section of the* Resources Library.

TO PROVIDE FEEDBACK ON EITHER OR BOTH OF THIS GUIDE OR THE RESOURCES LIBRARY PLEASE SUBMIT COMMENTS AND SUGGESTIONS BY EMAIL TO info@metrolabnetwork.org.

Distinguishing Between Governmental and Proprietary Functions (Chapter 2 of Local Government Immunity to Lawsuits in North Carolina (2018) at https://www.sog.unc.edu/sites/default/files/course_materials/Handout%20for%20COA%20%282019%29.pdf; Sean Andrés Rapela, *The Ugly Truth About Cyber Insurance & Governmental Data Breaches*, 21 J. High Tech. L. 242 (2021) at https://bpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/5/1153/files/2021/01/Rapela.pdf; and Rebekah Luna, *Stranger Danger!: How Hackers Break Into School Databases to Steal Student Data, and What Legislatures Should Do About It*, 54 Tex. Tech L. Rev. 381 (2022) at https://ttu-ir.tdl.org/handle/2346/90528.