MODEL DATA HANDLING POLICY FOR MUNICIPALITIES

ANNOTATED WORKING DRAFT 9-12-2019

Preamble: Origin, Purposes, Scope, and Crowdsourcing of Draft Policy

Origin of this Draft Policy:

Students and faculty in an interdisciplinary and multi-institutional projects-based, graduate-level course at the University of Missouri-Kansas City (UMKC) developed this draft Model Data Handling Policy (the "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 this draft reflect: (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;[2] (ii) research on several legal issues presented by municipal data initiatives; and (iii) review of a sampling of data sharing agreements that some cities have entered into with for-profit companies and other organizations in varying contexts.

Purposes and Scope:

The draft Policy contemplates (i) protecting privacy and other rights of individuals and entities as part of a duty of care in a municipality in the United States for the well-being of the public it serves, and the protection of the public commons, while (ii) also pursuing opportunities to provide public benefits from data gathering, data analytics, and data-driven provision of public services in a diligent and well-monitored manner.[3]

This working draft is in some respects aspirational. Collaborators who developed this document are mindful that a given city (of any size) considering adopting a Policy such as the one presented

[1] For a list of significant contributors to this draft Policy to date, see **Appendix 1** hereto. In addition, the Ewing Marion Kauffman Foundation supported some of the work on this draft Policy through a grant to UMKC for the Legal Technology Laboratory—see www.thelegaltechlab.com.

[2] We understand that relevant policies are developing rapidly across the country. While the students and faculty involved have studied several of them, there are doubtless others that have well-conceived and well-crafted provisions that might be instructive for future iterations of this draft Policy—so all reviewers of this draft are encouraged to in their feedback call attention to policies not referenced herein that they suggest be considered.

[3] *Cf.* Mission Statement of Data-Smart City Solutions, Harvard Kennedy School Ash Center for Democratic Governance and Innovation at https://datasmart.ash.harvard.edu/about/data-smart-city-solutions.

herein may face staffing and budgetary constraints that might currently preclude it from implementing some of its elements. The hope is that cities will come to the realization that the magnitude of both the potential benefits and the potential risks of increasingly powerful data gathering, dissemination, and analysis tools calls for the financial and human capital investments needed to institute and maintain such elements.

This Policy covers data created, collected, and maintained by a municipal government (the "City") or by contractors or third parties on behalf of or in contractual collaboration with the City. As reflected in the definition of "Data" below, the Policy includes the handling of not just "open data," but also other data collected directly by the City or for the City by contractors or agencies.[4]

Intended Crowdsourcing:

We are sharing this discussion draft of the Policy for review, comment and suggestions with other universities and cities, including through the MetroLab Network,[5] and other stakeholders. The goal is to essentially "crowdsource" further development of this draft Policy. We seek to gather feedback to inform and improve further iteration of the proposed principles, standards, guidelines, and practices for municipal "Data Handling" (as broadly defined below) that might be adopted by a jurisdiction in whole or in part, and with whatever modifications the jurisdiction deems appropriate for its particular circumstances. While some footnotes in this draft contain highlighted language urging reviewers to provide input on specific issues, we invite all reviewers to offer input on any provisions or discussions in the text and footnotes in this draft, as well as on any omissions of topics in this draft they feel should be included in the Policy.

Disclaimer:

Nothing herein is intended or should be construed as legal advice or a legal opinion. Any municipality considering using all or any part of this draft Policy as a tool in developing its policies or practices should seek legal advice and legal opinions from its legal counsel.

Questions, Comments, and Suggestions Welcomed and Encouraged:

Please direct questions, comments and suggestions regarding this draft Policy to Professor Tony Luppino of the University of Missouri-Kansas City (UMKC) School of Law by email to luppinoa@umkc.edu or by phone at 816-235-6165.

---

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

[5] For information on the MetroLab Network, see https://metrolabnetwork.org/.

Table of Contents

SECTION I: DEFINITIONS

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

Applicable Third Party: A contractor or company employed, engaged, or contractually collaborating with the City in any one or more aspects of Data Handling.

Chief Data Officer: The City employee designated by the Controlling Authority to perform the functions of a "Chief Data Officer" set forth in Section VIII.

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 City on significant Data Handling matters in accordance with Section VIII 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 VIII.[6]

Controlling Authority: [City to insert specifics of its governance circumstances to fit with roles for Controlling Authority described in this draft Policy].[7]

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

Data: A subset of information, whether quantitative or qualitative, that is regularly maintained by, created by or on behalf of, and owned or licensed by the City in non-narrative, alphanumeric, or geospatial formats. Data are an asset independent of the systems or formats in which they reside.[8]

---

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

[7] The definition inserted should account for the possibility of "designees"—for example, if the City determined the primary authority for some decisions or actions assigned to the Controlling Authority should be the Mayor, the City Manager, or the City Council or similar body, but that some decisions should be handled by another person or body, there could be language included in the definition along the lines of "or the designee to which such authority assigned responsibility for the particular decision or action in question."

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

Data Security Policy: The "Data Security Policy" described in Section V.

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.[9]

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

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

Data Handling Oversight System: The processes and procedures set forth in Section VIII.

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 PII from Data.

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

[9] *Id.*

[10] Based on Current Kansas City Policy, Section 2-2130 KC, in Chapter 2 of its Code of Ordinances, available at http://cityclerk.kcmo.org/liveweb/Documents/Document.aspx?q=ZbIEEaWPo6OisPlcKCOiyJgzsuFZYaAt7l1ZlhWVfmxQni0CLNUzTHC4o9SX%2FyKhs2G5pT0vgAHYH95no1IkrQ%3D%3D (hereinafter "KCMO Open Data Policy").

research community, and other partners to make use of such Datasets in support of the program's goals.[11]

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

Personally Identifiable Information (sometimes herein referred to as "PII"): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[12]

Principal Data Handling Administrator: The 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.

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

Sensitive Data:[13] Information that the City 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.[14]

Sunshine Laws: All open meeting, 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 City are subject.

---

[11] Based on definitions in Seattle Policy, *supra* note 4, at page 1.

[12] Directly from General Services Administration, *Rules and Policies - Protecting PII - Privacy Act* November 18, 2015 at http://www.gsa.gov/portal/content/104256.

[13] It may be that a city would like other categories of Data defined in their Data Handling Policy. This draft Policy defines Open Data, PII, and Sensitive Data (the latter including PII). Reviewers of this draft are encouraged to offer suggestions on such other categories—for example, should there be a definition of "Protected Data" that differs from "Sensitive Data"? *Cf.* San Francisco's Citywide Data Classification Standard at https://sfcoit.org/datastandard (which includes categories for "Public", "Internal Use", "Sensitive", "Protected", and "Restricted" data).

[14] Based largely on University of North Carolina Information Technology Services definition available at https://its.unc.edu/security/sensitive-data/.

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

SECTION II: CORE PRINCIPLES AND CORE OPERATING RULES

The City, through its agencies, departments, and personnel designated to implement or administer its Data Handling activities, must, in carrying on such activities, exercise the diligence and care appropriate to:

A. Ensure that no City Data Handling activities conflict with the principle that every individual has an equal right to a healthy and safe environment;

B. Require that air, water, land, and food be of a sufficiently high standard that individuals in its communities can live healthy, fulfilling, and dignified lives;[15]

C. Seek to enhance, protect and preserve the digital and physical environments, and foster a culture that recognizes that the duty to do so rests on the shoulders of government, residents, citizen groups, educational organizations, and businesses alike;[16]

D. Comply with applicable Privacy Laws and otherwise preserve and protect the anonymity of individuals whose Data is knowingly or unknowingly collected, and ensure that no individual's right to privacy is abridged;

E. Comply with the requirements of applicable Sunshine Laws, provided that to the extent such laws provide optional means of compliance, select the compliant means that best protect and preserve the privacy of individuals;

F. Subject to prohibitive mandatory provisions of applicable Sunshine Laws, require that all PII be De-identified at source at the time of collection[17] except to the extent otherwise approved by the Controlling Authority and allowable under applicable law;

---

[15] Based in significant part on the *Principles for Regulation of Emerging Technology and Urging the City Administrator to Convene an Emerging Technology Working Group* embodied in Resolutions adopted in April, 2018 by the Board of Supervisors of the City of San Francisco; see https://sfbos.org/sites/default/files/r0102-18.pdf.

[16] *Cf.* Chapter One of San Francisco Environmental Code, in American Legal Publishing - Online Library, at http://library.amlegal.com/nxt/gateway.dll/California/environment/chapter1precautionaryprinciplepolicystat?f=templates&fn=default.htm&3.0=&vid=amlegal%3Asanfrancisco_ca&anc=JD_Chapter1.

[17] *See, e.g.,* Future of Privacy Forum materials regarding De-Identification at https://fpf.org/issues/deid/.

G. When feasible and permitted by applicable laws, the City and Applicable Third Parties who are collecting Data regarding individuals shall notify individuals in advance that such Data is being collected;[18]

H. Enforce the individual's right to know, through a general privacy policy and with more specifics available upon request, what PII City government and Applicable Third Parties have collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;[19]

I. Enforce the individual's right to "opt out" of allowing the City or an Applicable Third Party to disclose or sell their PII to third parties (or, for individuals who are under [INSERT AGE OF MAJORITY IN APPLICABLE STATE], the right not to have their PII disclosed or sold absent consent lawfully provided on their behalf by an authorized person);[20]

J. Enforce the individual's right to have City government and Applicable Third Parties delete their PII subject to such exceptions approved in accordance with this Policy and permitted by applicable law.

K. Enforce the individual's right to receive equal service and pricing from a business over which the City has regulatory authority, even if they exercise their privacy rights.[21]

L. Maintain a master Data catalog that lists all available Datasets being collected or stored by or on behalf of the City and of the processes by which such Data may be made available to any private parties or to the public;[22]

---

[18] Based somewhat on 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 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[19] Based on provisions in The California Consumer Privacy Act of 2018—see PRIVACY LAW BLOG (2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/. *See also* NYC Guidelines for the Internet of Things at https://iot.cityofnewyork.us/.

[20] Based on provisions of The California Consumer Privacy Act of 2018. Reviewers of this draft are encouraged to offer examples of "opt out" provisions and of related disclosures of the implications of opting out or not opting out designed to help the individual makes a well-informed decision.

[21] *Ibid.*

[22] Maintaining a master Data catalogue is big task. However, the diligence required to properly classify and handle Data calls for a City to have a firm grasp on what Data/Datasets it has. Reviewers of this draft are encouraged to offer suggestions about protocols and standards might be need to make this task manageable. *Cf.* San Francisco Data Management Policy, Section 1.0 (Database and Data Inventories) available at https://sfcoit.org/datamanagement.

M. Emphasize and maintain transparency with the public on the usage and collection of Data where it is prudent and reasonable;[23] and

N. Ensure that the City's Data Handling practices comply with all requirements of applicable laws regarding the security, retention and disclosure of electronic Data.

SECTION III: SPECIAL PROVISIONS FOR OPEN DATA PROGRAMS

With respect to all of its Open Data Programs, the City shall:

1. Make Data it collects discoverable and accessible to the public only through Data Platforms that comply with this Policy;[24]

2. Assess the Datasets to publish as Open Data, in accordance with standards and procedures established from time-to-time by the Data Handling Oversight Committee, 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 therefor, and make the request, decision, and rationale for such decision 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 Handling 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;

[23] Based in part on City of Charlotte, *Open Data Policy* Jan. 1, 2015, at page 1, available at http://charmeck.org/maps/Documents/OpenDataPolicy.pdf. *See also* NYC Guidelines for the Internet of Things at https://iot.cityofnewyork.us/.

[24] Based on Washington D.C. *District of Columbia Data Policy* available at https://octo.dc.gov/page/district-columbia-data-policy.

6. Provide to the Data Handling Oversight Committee an annual "Open Data Plan" and annually report on the assessment of progress towards achievement of the goals described in the Open Data Plan for the previous year;

7. Include in its Open Data portal and any similar City-maintained mechanism for publishing Open Data the Limitation of Liability and Indemnity Provisions in substantially the forms set forth in **Appendix 2**;[25] and

8. To the extent prudent and possible, and subject to the limitations and precautions provided for in this Policy, the City shall:

   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.

SECTION IV: PRIVACY AND CONSTITUENT RIGHTS

A. The City's posted privacy policies and terms of use relating to Data Handling and Data portals shall be consistent with the Core Principles and Core Operating Rules set forth in Section II and the other provisions of this Policy.

B. In its collections and disseminations or releases of Data to persons or entities other than City employees or agencies, the City shall:

   1. Provide public notice available to the affected person about the collection, use and sharing of personal information at the time of such collection. This includes instructions about opting out of this collection, whenever reasonably feasible;

[25] *See* 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."

2. 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 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 he collection of such Data;

3. Adhere to the Data retention schedule recommended from time-to-time by the Data Handling Oversight Committee and approved by the Controlling Authority and dispose of or De-Identify information as required by such retention schedule;

4. Maintain public documentation explaining privacy practices that are in compliance with this Policy; and

5. Provide individuals with the opportunity to correct Data inaccuracies.[27]

SECTION V: SECURITY AND AUDIT MECHANISMS

A. Data Security Policy.

The City shall adopt a formal, written **"Data Security Policy"** for establishing and communicating data security requirements across all City departments and agencies. The Data Security Policy shall:

1. Classify all Data provided to, collected by or derived by the City or its representatives or contractors as either Open Data or Sensitive Data (mutually exclusive);

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

[26] As in note 20 above, it seems to many collaborators on this draft that new approaches are needed to develop better approaches to meaningful informed consent to capturing and use of personal data—and that approaches beyond clicking "accept" to complex/dense description in terms of use may well be in order. Reviewers of this draft are encouraged to include in their feedback ideas they have and studies or examples they have seen on this matter.

[27] *Cf.* Seattle Open Data Policy, *supra* note 4.

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

4. 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;

5. Require Data security training for (i) [CITY TO INSERT DESCRIPTION OF RANGE OF EMPLOYEES TO RECEIVE SUCH TRAINING] and (ii) all personnel of Applicable Third Parties who will be handling Sensitive Data;

6. Maintain plans to remedy or mitigate violations of the Data Security Policy, and plans to respond to system failures and breaches;[28]

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

8. Require periodic updates to the Data Security Policy to ensure alignment with all applicable laws, regulations, and City objectives and plans.

B. Data Handling Systems.

All Data Handling Systems operated or used by the City, its representatives and Applicable Third Parties, or interconnected to the City's network or Data Handling systems (each a **"Covered Data Handling System"**) shall provide mechanisms for compliance with the City's Data Security Policy. Such mechanisms shall include, without limitation the following:

1. All Covered Data Handling Systems shall be subject to a security assessment and tested for vulnerability to unauthorized access or use prior to deployment.[29] If a Covered Data Handling System employs any means of credit card transactions or

[28] *Cf.* San Francisco City-wide IT focused –Disaster Preparedness, Response, Recovery, and Resilience Policy available at https://sfcoit.org/dpr3.
[29] *Id.*

interfaces with third party systems that employ such transactions, such Covered Data Handling System shall comply with the provisions of the Payment Card Industry (PCI) Data Security Standard;

2. The City shall take additional precautions with respect to all Internet-accessible Covered Data Handling Systems to safeguard against unauthorized information access or manipulation by outside actors. The Chief Data Officer shall from time to time promulgate a series of tests using up-to-date federal standards for information assurance in order to ascertain the security of all Covered Data Handling Systems against:

    a. Unauthorized access to data sources in order to access, alter, or erase Data;
    b. Malicious use of any internet technology designed to deceive or give misinformation to any users;
    c. Schemes to steal user information for unauthorized system use;
    d. Re-Identification of previously anonymous or De-Identified PII;[30] and
    e. 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.

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

C. Compliance.

The City's Data Security Policy and Data Handling Systems shall comply with all applicable laws, regulations and City policies and practices. The City shall comply fully with applicable Sunshine Laws.[31] Legal notices and copyrights shall be included for disclosure purposes.[32]

[30] *Cf.* San Francisco's DataSF Open Data Release Toolkit at https://datasf.org/resources/open-data-release-toolkit/.
[31] From City of Seattle Web Presentation and Accessibility Standards Version 3.0, October 2, 2012.
[32] *Id.*

D. Security Audits.

The City shall conduct a periodic **"Security Audit"** [CITY TO INSERT HOW OFTEN] 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 Covered 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 must be among those included in each Security Audit:

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

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

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

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

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

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

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

E. Web Presence Audits. The extension of the City'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 to incorporate Web Presence Audits into the Security Audit. The purposes of such Web Presence Audits are to ensure that the City and Applicable Third Parties are taking the necessary steps to:

1. Prevent the use of unauthorized tools;
2. Minimize damage to individual or entity reputation;
3. Maintain regulatory compliance;
4. Prevent information leakage;
5. Minimize risks of harm from insufficient social media governance;[33] and
6. Mitigate risks of unanticipated unintended consequences.

F. Network and Communications Systems Audits.[34]

The City shall audit its network, including all interfaces and interconnections with third party networks and infrastructure, and its communications systems, whether controlled internally or

[33] *See* Michael Juergens, *Social Media Risks Create an Expanded Role for Internal Audit*, The Wall Street Journal, August 6, 2013 available at. http://deloitte.wsj.com/riskandcompliance/2013/08/06/social-media-risks-create-an-expanded-role-for-internal-audit/ for discussion of this and other areas of precaution listed immediately above.

[34] A city may want to expressly adopt specific standards for these types of audits and cross-reference or attached them as appendices their Data Handling Policy. Several potential relevant standards exist—for example see: cyberframework assessment and auditing standards and policies published by the National Institute of Standards and Technology (NIST); ISO 27001 (Information Security Management) and ISO 27002 (Security Techniques/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 available at https://sfcoit.org/cybersecurity. Reviewers of this draft are encouraged to include in their feedback the extent to which they feel specific auditing standards should be adopted in a city's Data Handling Policy, particular standards a city might consider, and principles of modifying adoption of standards as technology progresses and new standards evolve.

purchased as a service, for compliance with the City's Data Security Policy. The "Network and Communications Systems Audit" shall ensure that the City's network and communication systems:

1. Adhere to stated policies adopted by the City;
2. Maintain regulatory compliance;
3. Follow policies designed to minimize the risk of hacking or phreaking;[35];
4. Prevent information leakage; and
5. Mitigate risks of unanticipated unintended consequences.

SECTION VI. PROCUREMENT & RESPONSIBILITIES OF CONTRACTING PARTIES

A. Procurement Processes and Associated Guiding Principles[36]

The City's legal, organizational, technological, and training measures relating to the procurement of goods and services involving one or more aspects of Data Handling **("Data Handling Procurements")** must comply with its duty to make reasonably informed decisions that, to the greatest extent possible, protect the fundamental interests of the people that it serves. Diligent adherence to this Policy when planning to collect, store, secure, and make Data available through Data Platforms, including, without limitation, through Open Data Programs and formats, is the responsibility of all City personnel and Applicable Third Parties in order to safeguard the interests of the people that technology is designed to benefit.[37] Accordingly, Data Handling Procurements, and related requests for proposals **("RFPs")**, requests for information **("RFIs")**, and requests for quotes **("RFQs")** shall reflect adoption by the City of the following guiding principles:

1. The City shall recognize that the products and services it buys have inherent

[35] *See* definition at https://en.wikipedia.org/wiki/Phreaking.

[36] The following guiding principles for Data Handling Procurements are based to some extent on learning from information gleaned from ordinances found in Kansas City, Seattle, and San Francisco: see Ord. No. 150865, § 1, 10-22-15 (Kansas City); http://www.seattle.gov/Documents/Departments/FAS/PurchasingAndContracting/Purchasing/green_SustainablePurchasingPolicy.pdf (Seattle); and http://library.amlegal.com/nxt/gateway.dll/California/environment/chapter1precautionaryprinciplepolicystat?f=templates&fn=default.htm&3_0=&vid=amlegal%3Asanfrancisco_ca&anc=JD_Chapter1 (San Francisco).

[37] Cf. NYC Guideline for the Internet of Things at https://iot.cityofnewyork.us/operations-and-sustainability/.

social, human, health, environmental and economic impacts, and that the City should accordingly make procurement decisions that embody, promote and encourage a commitment to sustainability;

2. City personnel shall recognize their role in the City's duty to enhance, protect and preserve the environment. These responsibilities rest on the shoulders of government, Applicable Third Parties, residents, citizen groups, and businesses alike;

3. Due diligence in identifying and prohibiting or managing conflicts of interest, and in seeking to prevents or mitigate harm or inequity resulting from Data Handling; and

4. To the extent deemed applicable by the Controlling Authority in the particular request regarding a Data Handling Procurement, requiring that the responder address how they would address adherence to the one or more of the Core Principles and Core Operating Rules set forth in Section II above.

B. Negotiation of Data Sharing Agreements with Applicable Third Parties.

The Controlling Authority, with input from a Data Handling Oversight Committee, shall direct with respect to all Data Handling Procurements and all agreements with significant Data sharing elements **("Data Sharing Agreements")** to which the City is to be a party that the processes and protocols regarding Data Handling provisions in agreements with Applicable Third Parties set forth in this Section VI.B be followed.

1. ***Pre-signing Negotiation Checklists***:

   Included as **Appendix 3a** to this Policy are Pre-signing Negotiation Checklists regarding proposed contracts with the following three distinct types of vendors:

   a. **"Substantial Vendors"** offering substantial services in Data Handling (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 City);

   b. **"Specific Data Analytics Vendors"** offering services in specific data analytics (generally persons and entities that deal with Datasets more limited in nature than Substantial Vendors); and

c. **"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 City, in circumstances that are likely to produce significant Data that could be productively used by the City in a manner consistent with the Core Principles and Core Operating Rules set for in this Policy—for example, there might be productive open data exchanges negotiated to provide public benefits.

The relationship between a particular vendor and the City will often be unique based on the services offered by the vendor and goals of both the vendor and the City. However, there may be significant overlap in the way in which these entities approach agreements regarding the collection, protection, and dissemination of data. The Pre-signing Negotiation Guidelines forms attached in **Appendix 3a** are designed to take such variations into account and promote adherence by the City and Applicable Third Parties with this Policy, and must be completed for all Data Sharing Agreements to which the City is to be a party.

2. Post-signing Evaluation Reports:

a. City Reports. Included as **Appendix 3b** to this Policy are Post-signing Evaluation Report forms for the same three categories of vendors identified in B.1 above. The purpose of the Post-signing Evaluation Report forms is to give all parties to a Data Sharing Agreement in which the City is a party the opportunity to evaluate how well the agreement addressed the goals of each party, and whether there are areas of concern to the City that may be addressed in subsequent agreements either between the same parties, or by the City in similar agreements with different vendors. Subject to the timing provisions in c. below, the City shall produce a Post-signing Evaluation Report for each Data Sharing Agreement made after the effective date of this Policy.

b. Applicable Third Party Reports. The City should consider requiring the completion and sharing with the City of a Post-signing Evaluation Report by each Applicable Third Party that is a party to a Data Sharing Agreement, and providing for the sharing of such Post-signing Evaluation Reports among all parties to such agreement unless it is determined that one or more parties may use their report primarily for internal purposes and is not required to share it with the other parties.

c. **Timing of Post-signing Evaluation Reports.** The timeframe for completion of a Post-signing Evaluating Report described in a. or b. above for an executed Data Sharing Agreement may vary among applicable agreements, but should in no event end later than one year after the date of execution of the agreement. If the term of the applicable agreement will extend beyond one year, the agreement must be evaluated on an at least annual basis from the date of execution.

C. Responsibilities of Applicable Third Parties.

In negotiating Data Handling Procurements and Data Sharing Agreements, the City shall require that:

1. Each Applicable Third Party involved in one or more aspects of Data Handling be responsible for all equipment and infrastructure they deploy or any Data that they collect, store, share, transfer or over which they otherwise exercise dominion.

2. The City shall not be liable for loss or damages from the compromise of any Data or Datasets occurring while not in the possession of the City. The Applicable Third Party shall be responsible for the loss or damages caused by the compromise of Data or Datasets while in the possession of the Applicable Third Party.

3. Data in possession of an Applicable Third Party must be protected by a reasonable degree of care by the Applicable Third Party. Any and all liabilities resulting from or in connection with mishandling, misplacement, or abuse of such Data or Data sets therefore shall be the responsibility of the Applicable Third Party. Applicable Third Parties who will be subcontracting work or procuring goods or services from other vendors in connection with their performance under their agreements with the City shall require such subcontractors and vendors to similarly comply with the provisions of this paragraph regarding care with regard to Data protection.

To ensure compliance with the foregoing provisions of this Section VI, and otherwise to effectuate the principles and practices contemplated by this Policy, the City shall, in the negotiation and entering of any agreement with a prospective Applicable Third Party, follow the due diligence and process guidelines embodied in **Appendices 3a and 3b** hereto.

D. Coordination with Legal Counsel.

The appropriate City officers will work in collaboration with the City's Law Department and/or the City's other legal counsel in complying with the foregoing provisions of this Section VI in the course of all Data Handling Procurements and the negotiation and evaluation of all Data Sharing Agreements to which the City is or will be a party.[38]

VII. LIABILITY LIMITATIONS, SOVEREIGN IMMUNITY, AND CYBER-INSURANCE

A. Liability Limitation Measures.

The City shall in its Data Handling activities adhere to Terms of Use, Exclusion of Warranties, and Limitation of Liability and Indemnity Provisions in substantially the forms set for in **Appendix 2**, subject to modification from time to time directed by the Controlling Authority after consultation with the Data Handling Oversight Committee.

B. Sovereign Immunity and Cyber-insurance.

To the extent, if any, that the City's Law Department determines that Sovereign Immunity does not apply to any part(s) of the City's Data Handling endeavors, the City shall consider purchasing an appropriate cyber-insurance policy for coverage related to loss or damage resulting from a Data hack/breach or spillage of Data.[39]

VIII. DATA HANDLING OVERSIGHT SYSTEM

A. Purpose of the Oversight System.

The purpose of the **"Data Handling Oversight System"** is to provide a consistent process, with checks and balances, for the oversight of all aspects of Data Handling by the City and Applicable Third Parties and associated measures for the proper handling of Sensitive Data.[40] The City shall adopt, implement, and maintain mechanisms for oversight of Data Handling to ensure

[38] *Cf.* San Francisco Data Management Policy, Section 3.02 available at https://sfcoit.org/datamanagement.

[39] If a given city activity is deemed to not be part of a "governmental function," but instead part of a "proprietary" or other non-governmental function, sovereign immunity might not be available. An analysis of this issue may be in order, for example, if a city were to consider selling or making available to private companies Data or Datasets to generate revenues for the city. Determinations of whether and when sovereign immunity is available, and whether and when cyber-insurance is appropriate, are among the issues for a city's legal counsel to address.

[40] Based somewhat on DataSF.org: Open Data Release Toolkit pp. 2 (2016), available at https://datasf.org/resources/open-data-release-toolkit/.

compliance with the foregoing provisions of this Policy, which shall include, without limitation the processes and procedures described in the following provisions of this Section VIII.

B. Roles and Responsibilities of City's Primary Data Handling Personnel.

1. **Controlling Authority.** The Controlling Authority shall have ultimate authority over Data Handling by the City, but shall designate a Chief Data Officer to oversee all significant aspects of Data Handling and compliance with this Policy on a day-to-day basis,[41] and also appoint an Open Data Manager who shall oversee the implementation and management of the City's Open Data Programs and related policies and infrastructure.

2. **Chief Data Officer.**[42] The roles and responsibilities of the Chief Data Officer include:[43]

    a. Managing the safeguarding of the City's Sensitive Data;

    b. Ensuring that the provisions of Section V of this Policy, including, without limitation the tests and audits described therein, are implemented.

    c. Help City departments and agencies to make better use of available Data;

    d. Connect citizens with City Data to promote public benefits;

    e. Maintaining and keeping up-to-date systems designed to ensure compliance with Privacy Laws and Sunshine Laws;

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

    g. Coordinating with [INSERT CITY-SPECIFIC TITLES FOR ROLES OFTEN REFERRED TO AS "Chief Innovation Officers", "Chief Information Officers", and "Chief Technology Officers"] and all Unit Data Stewards and creating systems and

[41] *See, e.g.,* ongoing compilation on "WHO ARE AMERICA'S CHIEF DATA OFFICERS?" preliminary list on website of Data-Smart City Solutions, Harvard Kennedy School Ash Center for Democratic Governance and Innovation at https://datasmart.ash.harvard.edu/news/article/data-leadership-at-the-executive-level-761.

[42] Many organizations have established a "Chief Privacy Officer" (or similar position focused on privacy and related security issues). A city might what to consider creating such a position and assigning the Chief Privacy Officer primary responsibility for some of the duties listed in the following definition of Chief Data Officer.

[43] Several 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.

structures that promote teamwork and feedback loops to help reap the benefits of Data gathering and analytics in a manner consistent with this Policy, and in accordance with consistently applied quality assurance, accountability, and ethical standards.[44]

3. **Open Data Programs Manager.** The Open Data Programs Manager shall manage the City's Open Data Program, and in performing that function:

   a. Coordinate the publication of public data from City departments, agencies and commissions on the City's Open Data portal;[45]

   b. Be responsible for completion of all actions and reports required with respect to the City's Open Data Programs under Section III of this Policy.

4. **Unit Data Stewards.** The Chief Data Officer will designate a Unit Data Steward for each City department and agency (each a **"Unit"**), in each case in consultation with the Unit. A Unit Data Steward must be a City 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:

   a. Developing and maintaining a concrete understanding of (i) the inner workings and outer relationships of the Unit with regard to 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 Sunshine Laws that may apply to the Unit's Data Handling;

   b. 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; and

---

[44] *Cf.* San Francisco Data Management Policy at https://sfcoit.org/datamanagement and Citywide Data Classification Standard at https://sfcoit.org/datastandard (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").

[45] *Cf.* Section 2-2134 of the KCMO Open Data Policy at http://cityclerk.kcmo.org/liveweb/Documents/Document.aspx?q=ZbIEEaWPo6OisPlcKCOiyJgzsuFZYaAt7l1ZlhWVfmxQni0CLNUzTHC4o9SX%2FyKhs2G5pT0vgAHYH95no1IkrQ%3D%3D.

c. 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.

C. Data Handling Oversight Committee.

The "Data Handling Oversight Committee" will be comprised of the Chief Data Officer, the Open Data Programs Manager, all of the Unit Data Stewards, and the CAB "Convener" described in D. below, and have the following authority, responsibilities and general operating rules:

1. Oversee adherence to all elements of this Policy, including, without limitation, making recommendations to the Controlling Authority on matters on which the provisions of this Policy expressly allow for optional means of compliance or expressly contemplate discretionary actions;

2. Recommend to the Controlling Authority modifications of this Policy as and when the Committee deems such modifications in order to better adhere to the Core Principles and Core Operating Rules set forth in Section II or as development in technology or other circumstances necessitate such modifications to facilitate such adherence.

3. Review all audit reports generated pursuant the provisions of Section V of this Policy and make any recommendations to the Controlling Authority the Committee deems appropriate based on such reports.

4. Periodically review the City's training programs relating to Data Handling and provide recommendations to the Controlling Authority with regard to such programs.

5. Provide advisory input to the Controlling Authority on other matters or decisions regarding Data Handling on which it is asked to provide such input by the Controlling Authority or by the Community Advisory Board (CAB);

6. In all of 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 Controlling Authority; and

7. Hold regular meetings, at least once monthly, to facilitate performance of its functions and hold special meetings, whenever the Controlling Authority 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 Core Principles and Core Operating Rules set forth in Section II.

D. Community Advisory Board (CAB).[46]

1. **Composition of the CAB.**

   a. The "Community Advisor Board (CAB)" shall consist of a "Convener," who shall be a non-voting *ex officio* member of such Board, and [CITY TO INSERT NUMBER] regular Board members. The regular Board members shall represent diverse city stakeholders. Accordingly, efforts shall 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.

   b. Subject to d. below, The Convener shall be an individual designated by [CITY TO INSERT PROCESS, TERM LIMITS, ETC.].[47]

   c. Subject to d. below, the regular Board members shall be individuals designated by [CITY TO INSERT PROCESS, TERM LIMITS, ETC.].[48]

   d. In no event shall 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).

[46] 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 Model Data Handling Policy project through several semesters of the interdisciplinary Selected Projects in Law, Technology, and Public Policy course at UMKC. A regional approach to the CAB might be efficient and appropriate in many regions—i.e., one independent body that could help gather and channel informed and timely input from multiple community stakeholders to Data Handling decision makers or a city advisory board in any city in the region.

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

[48] A question to consider here is whether the Board members could/would be unpaid volunteers.

2. **Functions of the CAB.**

   a. The CAB's primary function shall be to provide the Data Handling Oversight Committee with informed, timely, and diverse community input and recommendations on City Data Handling matters and decisions (i) on which the Data Handling Oversight Committee requests such advisory input and (ii) that the CAB determines should be brought to the attention of the Data Handling Oversight Committee.[49]

   b. In performing its primary function, the CAB shall seek to (i) advance adherence to the Core Principles and Core Operating Rules set forth in Section II, and (ii) develop systems and methods for gathering, memorializing, and reporting to the Data Handling 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");

   c. The CAB shall also collaborate with the Community End User Testing Group described below to facilitate diversity and timeliness in participation by community stakeholders in that Group's work.

   d. The CAB shall have regular meetings, no less frequently than [CITY TO INSERT], as well as special meetings when called by the Convener (with notice reasonable in the circumstances presented. The CAB shall fix its own operation rules and procedures in manner appropriate for its above-described functions.

2. **Functions of the Convener.**

   a. The Convener shall:

   (i) Present an annual budget for the CAB to the City Council (or equivalent authoritative body) 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 as and when needed;

[49] *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.").

(iv) Administer the conduct all CAB meetings;

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

(vi) Serve on the Data Handing 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; and

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

E. Civic End User Testing Group.[50]

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

1. The CEUTG shall 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.
2. The City will 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.
3. The City may incentivize participation in the CEUTG testing by providing testers with small monetary awards for completing applications and testing.[51]
4. The CEUTG shall report feedback from its user testing activities directly and simultaneously to the Data Handling Oversights Committee and the CAB.

---

[50] *Cf.* Chicago Tech Collaborative CUTGroup described at https://www.citytech.org/civic-design and background at https://cct.org/about/partnerships_initiatives/smart-chicago-collaborative/ and *KC Digital Drive, Code for KC and Missouri Western University launch Kansas City's first civic UX testing group.* 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)

[51] 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.

[CITY TO INSERT PROCDURES RE: PROPOSED AMENDMENTS]

[CITY TO INSERT PROCEDURAL INFORMATION AND SIGNATURE BLOCKS]

APPENDIX 1: SIGNIFICANT CONTRIBUTORS TO THIS DRAFT POLICY

[TO BE INSERTED IN SUBSEQUENT DRAFT]

APPENDIX 2: LIMITATION OF LIABILITY AND INDEMNITY PROVISIONS

[CITY TO INSERT TERMS OF USE/EXCLUSION OF WARRANTIES/OTHER RELEVANT LANGUAGE]

APPENDIX 3: NEGOTIATING/EVALUATING AGREEMENTS WITH THIRD PARTIES

In connection with Section VI.B of this Policy:

Appendices 3(a)(1), 3(a)(2), and 3(a)(3) below contain forms for Pre-signing Negotiation Checklists to be used by City personnel, with input from the City's Legal Department, in negotiating Data Sharing Procurements with Applicable Third Parties of the three types described in Section VI.B of this Policy: Substantial Vendors, Specific Data Analytics Vendors, and Miscellaneous Vendors.

Appendices 3(b)(1), 3(b)(2), and 3(b)(3) below contain forms for Post-signing Evaluation Reports to be used by the City with regard to applicable agreements with those same three categories of vendors, and, as contemplated in Section VI.B, may also be required to be completed and shared with the City by such vendors.

APPENDIX 3(a)(1): Pre-signing Guidelines for Substantial Data Handling Partner Contracts:

Purpose: The purpose of this checklist is to provide an applicable City official with guidance on important considerations when negotiating a contract involving the storage, distribution, ownership and usage of Data by a "Substantial Vendor" offering substantial services in Data

Handling (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 City).

Instructions:

1. As used herein, "Contract" means the *proposed* agreement being negotiated with a Substantial Vendor.
2. To help ensure that the Contract contains necessary aspects, from the City's perspective of a Data handling contract between a collaborative vendor and municipality, it is imperative that the City official(s) with the authority to negotiate the Contract prepare or obtain a draft of the proposed Contract in circumstances that make it clear there are not yet any binding agreements as to its terms.
3. Once that draft is available, the applicable City official(s) must include utilization of this checklist to develop a list of strengths and weaknesses within the Contract.
4. If any of the following boxes cannot be checked as completed because the element described has not been addressed or resolved, the applicable City official(s) should highlight those points, so they can be raised during further negotiations.
5. A few questions below will ask for the applicable City official(s) to reach an opinion or judgment. The City official(s) should consult with the City Law Department or, if applicable, outside legal counsel (whichever, "Applicable Legal Counsel") as necessary or appropriate throughout the Contract negotiation process.
6. If unsure whether an element listed below has been properly addressed in the pre-signing negotiations, the City official(s) should ask the vendor how such vendor intends to satisfy its obligations relating to such element during negotiations and discuss the response with Applicable Legal Counsel.

Negotiation Checklist:

A. The Basics:

- ☐ Each party involved in the Contract has been named
  - ☐ One or more City officials have been authorized to negotiate and sign the Contract if it is approved by the appropriate City authority(ies)
  - ☐ Collaborative vendor representative or point of contact for Contract is identified
  - ☐ All persons or entities other than the City and the vendor that will have any obligations with regard to this Contract ("Other Obligors") have been identified.
- ☐ Contact information (mailing address, email and phone number) for all parties
  - ☐ Obtained re: City official(s) in charge of negotiations/signing the Contract
  - ☐ Obtained re: Collaborative vendor representative or point of contact for Contract obtained
  - ☐ Obtained re: each Other Obligor (if any)

- ☐ The Contract has a defined termination date or a clear method of determining it
- ☐ The Contract has a renewal option beyond initial term
  - ☐ No
  - ☐ Yes
  - ☐ If there is a renewal option, the Contract clearly states the terms of the option (e.g. which party or parties have the option, and what is required to exercise it)
- ☐ The Contract clearly outlines how the vendor will be compensated
  - ☐ The vendor's price will not change or fluctuate unless otherwise expressly contemplated in the agreement or subsequently agreed to in writing by the City

B. Adherence to Core Principles and Core Operating Rules; and Due Diligence

- ☐ In the opinion of the City official(s) charged with negotiating the Contract, the Contract is consistent with the Core Principles and Core Operating Rules set forth in Section II of the City's Data Handling Policy, and contains provisions on the ownership, sharing and use of Data that advance adherence to those Core Principles and Core Operating Rules.
- ☐ The primary purpose of the goods or services to be provided by the Substantial Vendor are clearly outlined in the Contract and the City official(s) charged with negotiating the Contract either possesses or has accessed on behalf of the City the requisite technical expertise to determine that:
  - ☐ Due diligence has been done demonstrating that the Substantial Vendor is capable of fully performing its obligations under the Contract
  - ☐ Other Substantial Vendors were considered as alternatives to the Substantial Vendor named in the Contract and a reasoned decision was made to engage the Substantial Vendor for this Contract
  - ☐ There is sufficient clarity on the substance of the Substantial Vendor's obligations under the Contract to allow the City, through one or more of its employees or anticipated consultants, to monitor and assess the Substantial Vendor's performance of its obligations under the Contract

C. Relationships to Substantial Partner

- ☐ After due diligence it has been determined that the Substantial Vendor has in the proposed Contract proposed a standardized approach to providing the services or goods that is substantially the same as it has taken in similar contracts with other cities.
  - ☐ If not, the Contract clearly outlines how the approach is specifically tailored to the City's needs

D. Control and Access of Data Being Collected, Owned, and Used

- ☐ There is a definition of the Data being collected
  - ☐ If there are multiple types of Data being collected, there is a definition for each type of Data
  - ☐ Each definition describes how the Data will be collected and stored
  - ☐ The definition of Data has been reviewed and approved on behalf of the City by a person with the requisite technical expertise to conclude that eah such definition is appropriate
- ☐ The Contract expressly lists which entities (City, vendor, third party, etc.) have access and control over the Data (or each type of Data if applicable).
- ☐ The process by which Data may be accessed or controlled is clearly explained in the Contract.
- ☐ There are clear provisions on the ownership of and use rights with respect to the Data being collected under the Contract, and such provisions are consistent with the Core Principles and Core Operating Rules set forth in Section II of the City's Date Handling Policy

E. Storage of the Data and Security Measures

- ☐ The Contract contains clear provisions as to how, where, and under whose control the Data will be stored and secured consistent with the provisions of the City's Data Handling Policy
- ☐ The Contract provides options for the data to be stored in multiple formats
  - ☐ Each format, if applicable, is defined in the Contract
- ☐ The Contract defines how often Data will be gathered and stored (i.e. daily, weekly, monthly, quarterly etc.)

F. Data Breach

- ☐ The Contract defines what constitutes a Data breach.
- ☐ The Contract outlines the appropriate protocol each party should take if a data breach were to occur
  - ☐ The entities responsible for communicating with the authorities are listed
  - ☐ The individuals from each party that will form a response team are identified
  - ☐ The protocol for any unaffected Data and any backups is clearly outlined in the Contract

G. Monitoring Performance Under the Contract

- ☐ The Contract clearly addresses how the parties will implement their respective performance after it is signed, including, as applicable, reporting and monitoring obligations
- ☐ The Contract identifies which individuals (or offices) will oversee such implementation, reporting, and monitoring

H. Breach of Contract

- ☐ The Contract clearly defines ways each party could breach the contract
- ☐ The Contract clearly addresses remedies for breach of the Contract by each party
  - ☐ Sets forth on a party-by-party basis extent of liability, rights of other party(ies) to terminate the Contract due to a failure to perform/breach of a party's obligation, and has provisions on the exercise of associated rights by the non-breaching party(ies)

I. Legal Analysis/Approval

- ☐ The City's Legal Department has determined that:
  - ☐ After applying the City's conflict of interest rules, there are no conflicts of interest prohibiting the execution of the contract by the City or the Substantial Vendor
  - ☐ There would be no apparent legal violations by the City, the Substantial Vendor or any Other Obligor in executing or performing its obligations regarding the Contract
  - ☐ The Contract has been properly approved by the appropriate City authority.
  - ☐ None of the provisions of the proposed Contract regarding the nature of the Data being collected, or the manner in which the Contract contemplates such data will be stored, analyze, otherwise used and/or disseminated conflict with the Core Principles or Core Operating Rules in the City's Data Handling Policy

[INSERT APPROPRIATE SIGNATURE BLOCKS FOR CITY OFFICIAL(S) CHARGED WITH NEGOTIATING THE CONTRACT AND THE CITY LEGAL DEPARTMENT TO AFFIRM COMPLETION OF THE CHECKLIST]

[APPENDICES 3(a)(2) and 3(a)(3) TO BE INSERTED AFTER VETTING THE DRAFT OF 3(a)(1) WITH MULTIPLE COMMENTERS]

APPENDIX 3(b)(1): Post-Signing Evaluation Report for Substantial Vendor Data Handling Contracts

Purpose: The purpose of this evaluation reporting form is to help assess the results of Data Handling Agreements in a "Contract" between a City and a "Substantial Vendor" (i.e., a vendor providing substantial services in Data Handling (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 City). That assessments includes measuring the performance of such Contract against the Core Principles and Core Operating Rules set forth in Section II of the City's Data Handling Policy and the degree of adherence to other relevant requirements set forth in that Policy. Such measurements and assessment thereof can help inform the City in the negotiation of subsequent Data Handling Agreements with the same or other Substantial Vendors, and provide valuable information as it gauges the efficacy of its Data Handling Policy and considers possible modifications thereto.

NAME OF CONTRACT: _____

I. INFORMATION REGARDING PARTIES TO THE CONTRACT

A. Regarding the City:

1. Name of City: _____
2. Link to City's Data Handling Policy [INSERT]:
3. City Official(s) who were in charge of negotiating the Contract (write name in print and email) _____
4. Does the Contract or other documentation describe the City governance process followed for approval of the Contract and, if applicable, approval of amendments to the Contract? (If so, cite the relevant provisions and briefly summarize the process) _____

5. Is this a standard contract that the City uses with several vendors or was it modified for the Substantial Vendor in question?

    a. If applicable, explain how the standard contract was modified

_____

_____

B. Regarding the Vendor:

1. Name of Vendor: _____
2. Contact information for Vendor (email and phone):

_____

3. Link to Vendor's privacy and security policies regarding Data if applicable: [INSERT]
4. Does the Vendor (or any affiliate) have any other known contracts with the City? (If so, list such other contract(s))

_____

C. Regarding a Third Party—i.e., an Obligor on the Contract other than the City and the Substantial Vendor (if applicable):

1. Name of Third Party: _____
2. Contact information for Third Party (email and phone)

_____

3. What good or services does the Third Party provide?

_____

4. What are such Third Party's obligations regarding the Contract?

_____

5. What is the relationship of the Third Party to the Substantial Vendor?

   _____

6. What is the relationship of the Third Party to the City?

   _____

7. What entity is the Third Party obligated to report to (the Substantial Vendor, the City or both), and how often?

   _____

II. OTHER BASIC INFORMATION REGARDING THE CONTRACT ITSELF

A. Regarding the Type of Contract, its Term, and Compensation:

1. Is the Contract a public/private partnership collaboration agreement or a more limited vendor agreement? Explain why you believe the Contract is one over the other.

   _____

   _____

2. What is the nature of the goods/services the Vendor was required to provide under the Contract?

   _____

3. Does the Contract state that the Vendor was to be the exclusive provider of such goods/service to the City? _____

   a. If the Contract is silent on this provision, is there any evidence that a different Vendor or collaborator would have been able to provide similar goods/services? If so, which ones?

      _____

   b. If the Contract is silent on this provision, is there any evidence to indicate that third parties could have provided comparable goods/services?

      _____

4. What was the basic term (duration) of the Contract? _____

    a. Does the Contract contain provisions for termination by the City before the end of the stated term? (If so, described the circumstances allowing such termination).

    _____

    b. Does the Contract contain provisions for termination by the Vendor before the end of the stated term? (If so, described the circumstances allowing such termination).

    _____

5. Are there any renewal options? (If so, what are these options, and what are/were the durations of the option).

    _____

6. What is the manner of compensation to the Vendor under the Contract (fixed fee, contingent fee/percentage of revenues, other arrangement)?

    _____

    a. Did the Contract allow for the compensation to the Vendor to change or fluctuate?

    _____

    b. If the Contract was silent as to compensation fluctuations, has the compensation changed over time (and, if so, how were such changes approved)?

    _____

B. Regarding Data Ownership, Use, Security and Breaches:

1. List verbatim all relevant definitions of "data" in the Contract (e.g., City's Confidential or Proprietary Data; Vendor's Confidential or Proprietary Data; Sensor Data; End User Data; Personally Identifiable Information; or other defined categorizations of data).

    [INSERT HERE]

2. For each defined category of Data listed in 1 above, list below:

    a. The owner of the Data per the Contract.

    _____

b. The use and distribution rights of each party to the Contract (including applicable limitations/ conditions and purpose as to why data is being collected and shared).

_____

c. The extent of the ability of each party to the Contract to grant sub-use and/or distribution rights to third parties without needing the consent of the other party.

_____

d. If the Contract includes in text or in appendices specific data fields involved, list those.

_____

e. How was Data to be collected and stored per the Contract? What devices have been/are being used to collect it?

_____

3. Does the Contract contain provisions on to ensure compliance with applicable limitations/conditions on use of Data by one or more of the parties? (If so, briefly describe such provisions and supply a cross-reference to the applicable provisions in the Contract).

_____

4. Does this Contract allow the City to have Data access for educational, research or other purposes and, if so, under what conditions, and with what rights to share that access with contractors providing data analytics or other services to the City?

_____

5. Does the Contract prescribe Data security standards to be adhered to by the City? (If so, supply a cross-reference to the relevant provisions in the Contract)

_____

6. Does the Contract prescribe Data security standards to be adhered to by the Vendor? (If so, supply a cross-reference to the relevant provisions in the Contract)

_____

7. Does the Contract set forth processes/protocols that to address a Data breach (If so, supply a cross-reference to the relevant provisions in the Contract)

_____

8. Does the Contract expressly address the relative responsibilities of the parties for Data breaches? (If so, supply a cross-reference to the relevant provisions in the Contract)

_____

C. Other Notable Provisions:

1. Does the Contract contain provisions apart from those addressed above that pertain to risks, responsibilities, and rewards, or any other matters you feel are notable? (If so, briefly describe such provisions and supply cross-references to the applicable provisions in the Contract):

---

2. On a scale of 1 to 5, with 5 being very successful, please rate how well you think performance under this Contract to date has furthered the City's objectives in entering into this Contract with this Substantial Vendor _____

    a. Explain your basis for that rating:

    _____

    _____

3. On a scale of 1 to 5, with 5 being very successful, please rate how well you think performance under this Contract to date has been consistent with the Core Principles and Core Operating Rules set forth in Section II of the City's Data Handling Policy? _____.

    a. Explain your basis for that rating:

    _____

    _____

[INSERT APPROPRIATE SIGNATURE BLOCK(S) FOR CITY OFFICIAL(S) DOING THE POST-SIGNING EVALUATION OF THE CONTRACT]
