TED M. ROSS
GENERAL MANAGER
CHIEF INFORMATION OFFICER

MARYAM ABBASSI
ASSISTANT GENERAL MANAGER

BHAVIN PATEL
ASSISTANT GENERAL MANAGER

TITA ZARA
ASSISTANT GENERAL MANAGER

EDUARDO MAGOS
ACTING ASSISTANT GENERAL MANAGER

CITY OF LOS ANGELES

CALIFORNIA

KAREN BASS
MAYOR

ITA

INFORMATION TECHNOLOGY AGENCY

CITY HALL EAST
200 N MAIN ST, ROOM 1400
LOS ANGELES, CA 90012
213.978.3311

ita.lacity.org

October 9, 2024 REF: EXE-148-24

Honorable Members of the City Council
City of Los Angeles
Room 395, City Hall
Los Angeles, CA 90012

Attn: Government Operations Committee

Subject: **ARTIFICIAL INTELLIGENCE (A.I.) TECHNOLOGY, CITY GOVERNMENT USE, AND SERVICE ENHANCEMENTS (COUNCIL FILE 23-1020 - 10A)**

Pursuant to the amended Motion on Council File No. 23-1020, the Information Technology Agency is submitting the following report, including a City of Los Angeles Digital Code of Ethics, the Artificial Intelligence (A.I.) Safety Checklist for new A.I. tools, and the A.I. Tool Request Form, as described in the Los Angeles A.I. Roadmap previously submitted.

The following documents were developed in consultation with the Citywide Information Technology (IT) Policy Committee (ITPC), which is composed of IT managers and professionals representing all City departments, to build the necessary and important A.I. safeguards at the City of Los Angeles and for departments to adhere to when developing new A.I. tools and technologies.

1. **City of Los Angeles Digital Code of Ethics** - This document articulates City of Los Angeles' ethical standards, principles, and guidelines in the use of emerging technology, providing guidance to all City departments, including core values (Human-Centric, Equitable, Transparent, Secure, and Sustainable) and digital standards applicable to all LA City departments;

2. **Artificial Intelligence (A.I.) Safety Checklist** - This checklist was developed as a tool for departments to ensure due diligence and thoughtful examination before, during, and after the implementation of A.I. tools. This checklist will help City of Los Angeles Departments ensure that all A.I. tools adopted by the City of Los Angeles are implemented in as ethical, transparent, human-centered, and secure a process as possible.

3. **Artificial Intelligence (A.I.) Tool Request Form** - This form is developed for City of Los Angeles departments seeking to implement a new Artificial Intelligence (A.I.) Tool to request a review by the Information Technology Agency (ITA).

RECOMMENDATIONS

The Information Technology Agency's recommendation is to note and file this report.

IMPACT STATEMENT

No impact Statement.

Respectfully Submitted,

Ted Ross

Ted Ross
General Manager

Attachments: City of Los Angeles Digital Code of Ethics
Artificial Intelligence (A.I.) Safety Checklist
Artificial Intelligence (A.I.) Tool Request Form

ec: Matt Szabo, City Administrative Officer
Sharon Tso, City Legislative Officer
Matt Hale, Mayor’s Office
Dawn Comer, Mayor’s Office
Executive Team, Information Technology Agency

City of Los Angeles Digital Code of Ethics

Code of Ethics

Human-Centric

Sustainable

Transparent

Secure

Equitable

ACKNOWLEDGEMENTS

We would like to acknowledge the progressive leadership of Mayor Karen Bass and our other elected leaders: City Attorney Hydee Feldstein Soto, Controller Kenneth Mejia, and City Council, specifically Government Operations Committee Chairperson Imelda Padilla and Councilmembers Eunisses Hernandez and Heather Hutt who ask the tough questions and expect excellence from City of Los Angeles technology.

The lead author of the Digital Code of Ethics was General Manager Ted Ross with contributions in the emerging technologies section from Gartner Inc, Google, Microsoft Corporation, and the University of Southern California (USC). The graphics editors were Balmore Botero and Calvin Lee. Technology leaders from across the City of Los Angeles were instrumental in review and input through the citywide Information Technology Policy Committee (ITPC). The continued commitment to innovation and digital ethics by General Managers at the City of Los Angeles is both an inspiration across Southern California and around the world.

As the digital landscape is ever changing, this Digital Code of Ethics is a “living document.” As such, we thank the members of our Information Technology Policy Committee (ITPC) in advance who will review it annually to ensure it is up-to-date, incorporates new significant emerging technologies, and that it continues to align with our digital values.

TABLE OF CONTENTS

DIGITAL CODE OF ETHICS… AT A GLANCE

- The City of Los Angeles (L.A.) provides critical services to over 4 million residents, 50 million annual tourists, and 503,000 businesses.

- For over 230 years, L.A. sought innovative ways to improve our growing urban environment. This mission has been transformed by the Digital Age.

- The City of L.A. has been building world-class technology, recently earning the coveted #1 U.S. Digital City award & World Cities Summit Smart City award.

- However, digital innovation is not enough. As Americans become increasingly digital, they have also become increasingly distrustful of digital technology.

- The City of Los Angeles needs digital services that are both *innovative and ethical*. This is why we have drafted and adopted this Digital Code of Ethics.

- The Digital Code of Ethics articulates our ethical values, principles, and guidelines in the use of technology and data, providing guidance to all City departments.

- The values in our Digital Code of Ethics are derived directly from input from Los Angeles residents, business coalitions, elected officials, and local academics.

- Our principles and guidelines are based on five (5) core values for technology: Human-Centric, Equitable, Transparent, Secure, and Sustainable.

- These values are then reflected in ten (10) key digital principles:
    a. We build ethical technology, not just innovative technology
    b. Our technology must be both functional and easy to use
    c. Technology must enable transparent government
    d. Technology must increase accessibility for L.A. communities
    e. Technology must be built for the present and the future
    f. We do not sell personal data
    g. Your location is fundamental to your privacy
    h. Our technology respects user privacy
    i. We seek to hire a technology workforce as diverse as L.A.
    j. We invest in our communities to reduce the digital divide

- As emerging technology raises unique ethical dilemmas, we address them further through specific guidelines. Those technologies include Artificial Intelligence, Blockchain, Data Analytics, Digital Assistants, Drones, Facial Recognition, Healthcare Data, Internet of Things, Social Media, and Virtual/Augmented Reality.

- This Code of Ethics is a “living document.” Each year, our Information Technology Policy Committee (ITPC) will engage stakeholders, review, and make updates.

DIGITAL ETHICS: WHY IT MATTERS

"Technology continues to transform the ways we engage with information, organizations, and each other. But among the promise technology holds, there is the potential for harm. To promote the good and protect against unintended consequences we need *a new understanding* of what it means to create trustworthy and ethical technology."

-Deloitte, Technology Trust & Ethics, 2023

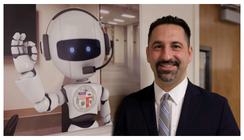
The City of Los Angeles provides critical public safety, economic development, transportation, public works, sanitation, and cultural services to over 4 million residents, 500,000 businesses, and over 50 million annual visitors. Angelenos rely on the 45 L.A. City departments to answer 9-1-1 calls, clean streets, fix potholes, remove graffiti, collect trash, and make it easier to work and play in Los Angeles. For over 230 years, L.A. City government has sought new, innovative ways to improve our growing urban environment and serve the needs of our diverse communities. In the last several years, this mission has been transformed by the Digital Age and the COVID-19 Pandemic. 90% of Americans own smartphones, 74% are active on social media, and 80% shop online (Pew Research Group, Mobile & Social Media Fact Sheets, 2024). In this digital era, Angelenos expect a lot from their L.A. City government. They want easy-to-use, powerful websites, apps, and A.I. digital assistants to request City services (fixing potholes, removing graffiti, repairing streets, etc) and get the information they need. Responding to these expectations, the City of Los Angeles has been building world-class technology to provide residents, businesses, and visitors with the secure digital services they expect from a leading global city. In fact, these efforts have been recognized, earning the coveted #1 U.S. Digital City award, a national Cybersecurity award, a Webby award for LACity.gov, and multiple international Smart City awards. However, innovation is no longer enough.

As Americans have become increasingly digital, they have also become increasingly distrustful of digital technology. From privacy concerns to data breaches, Americans are concerned that the innovations they use daily will have profoundly negative impacts on their lives. These anxieties have become so prominent that Oxford Dictionary officially added "techlash" (technology backlash) as a word in the English dictionary. This anxiety is only increasing with every new technological innovation. ChatGPT, for example, instantly became the fastest growing software application in human history, gaining 100 million users within the first two months, challenging social and legal standards for academic work, intellectual property, and the role human/computer interactions play in our society. As a government that heavily uses technology to serve our more than 4 million Angelenos, the City of Los Angeles understands the importance of digital services that are both *innovative and ethical*. This is why digital ethics matters at the City of Los Angeles.

Digital ethics is our code of conduct for electronic interactions with residents, businesses, and visitors. Drafted by the L.A. City Information Technology Agency, reviewed by many stakeholders and advocacy groups, and adopted by the citywide Information Technology Policy Committee (ITPC), this Digital Code of Ethics clearly articulates our ethical values, principles, and guidelines in the use of technology and data to interact with residents and perform City operations. Without these safeguards, our government risks alienating the very stakeholders that we serve. It has become imperative that ethical values and principles be identified and put in place to reinforce the public's digital trust. This is more than just compliance with existing laws; this is an update to our social contract in an increasingly digital world.

Since information technology (IT) has become such a predominant tool to engage L.A.'s residents and deliver City services, this Digital Code of Ethics was drafted to provide guidance to all City of Los Angeles departments, including specific guidelines in the use of emerging technologies (e.g. artificial intelligence, drones, blockchain). This is done to help deliver assurance to city residents & employees that the City of L. A. values their privacy and takes active measures to prevent unintended ethical consequences. The principles expressed in this Digital Code of Ethics are derived directly from resident feedback, community meetings, representatives of business coalitions, meetings with our elected officials, other municipalities, and academic experts in digital ethics. This includes experts from the University of Southern California, Sunlight Foundation, Open Government Partnership, Google, Microsoft, Gartner Inc., Data Ethics 4 All Foundation, other city governments, and more. Unlike private sector tech companies, the government is presumed to provide leadership in the responsible and ethical use of modern technology. At the City of Los Angeles, we understand that public trust takes time to build and can be easy to lose. Through this Digital Code of Ethics, the City of Los Angeles is committed to not only building innovative technology solutions, but understanding and controlling these technologies in a way that maintains the public's digital trust for years to come.

Ted Ross
General Manager and CIO
City of Los Angeles, Information Technology Agency



THE ROLES WE PLAY

“No one can whistle a symphony. It takes a whole orchestra to play it.”
-H. E. Luccock, American Professor & Author

Digital ethics is not the responsibility of one person or one group of people. We all play an important role.

Below is a summary of digital ethics roles at the City of Los Angeles:

A. **Los Angeles Residents & Advocacy Groups**
   a. Understand their digital rights
   b. Contact the City or an advocacy group (e.g. business associations, social welfare organizations, etc) with concerns about technology or data use

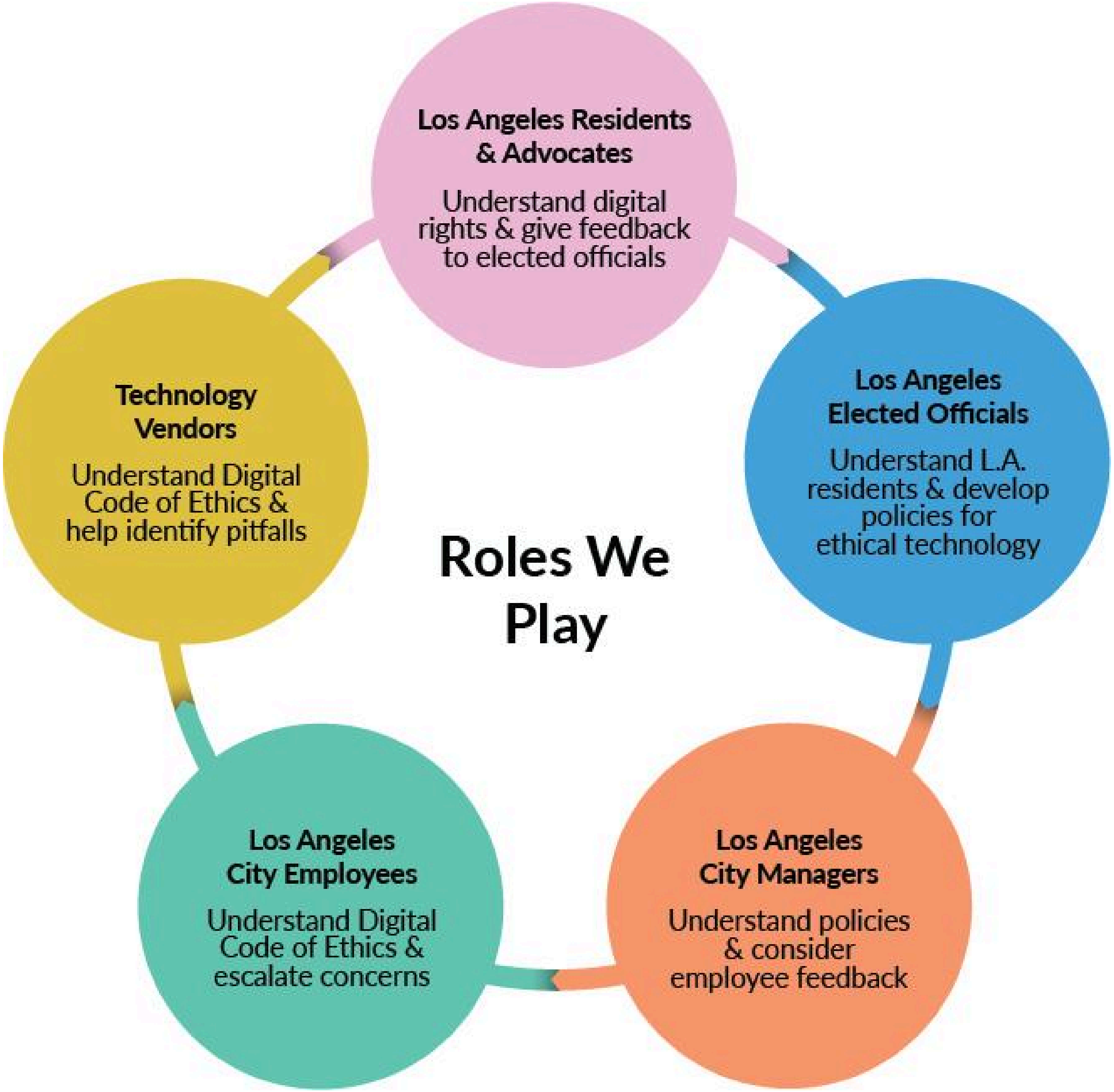
B. **Los Angeles Elected Officials**
   a. Develop and enforce policies for ethical use of technology
   b. Listen and respond to concerns of L.A. residents or businesses

C. **Los Angeles City Managers**
   a. Evaluate ethical consequences before choosing technology platforms
   b. Establish preventative measures to avoid digital ethics violations
   c. Provide feedback opportunities for employees or vendors to raise concerns
   d. Establish safeguards to ensure compliance with L.A. Digital Code of Ethics

D. **Los Angeles City Employees**
   a. Escalate ethical technology concerns up your chain-of-command
   b. Identify digital ethics concerns early in technology & data projects
   c. Adhere to L.A. Digital Code of Ethics when performing daily tasks

E. **Technology Vendors**
   a. Understand and adhere to the Digital Code of Ethics
   b. Assist City staff in identifying ethical concerns when choosing technology
   c. Recommend ways to prevent negative ethical consequences in technology
   d. Build and deploy ethical technology and data solutions for L.A. residents

Everyone Plays a Role in the City of Los Angeles



Roles We Play

Los Angeles Residents & Advocates

Understand digital rights & give feedback to elected officials

Los Angeles Elected Officials

Understand L.A. residents & develop policies for ethical technology

Los Angeles City Managers

Understand policies & consider employee feedback

Los Angeles City Employees

Understand Digital Code of Ethics & escalate concerns

Technology Vendors

Understand Digital Code of Ethics & help identify pitfalls

OUR DIGITAL VALUES

"71% of Americans are very concerned or somewhat concerned about how the government uses the data it collects about them."

-Pew Research Center, "Americans and Data Privacy Survey", 2023

Every year, technology changes. However, good guiding principles and values for technology do not. Beyond simply complying with federal and state laws, the City of Los Angeles Digital Code of Ethics is based on five fundamental values:

Value #1: Human-centric

Our technology and the resulting data is not just for the benefit of government operations, but fundamentally for the benefit of residents, businesses, and visitors in our communities.

Value #2: Equitable

Our public digital services should provide fair treatment and easy access by all of our diverse communities, and our technologies must not be used to discriminate against them.

Value #3: Transparent

We must never implement technology that we don't understand (no "black boxes") and will disclose the use of sensitive data through easy-to-understand policies.

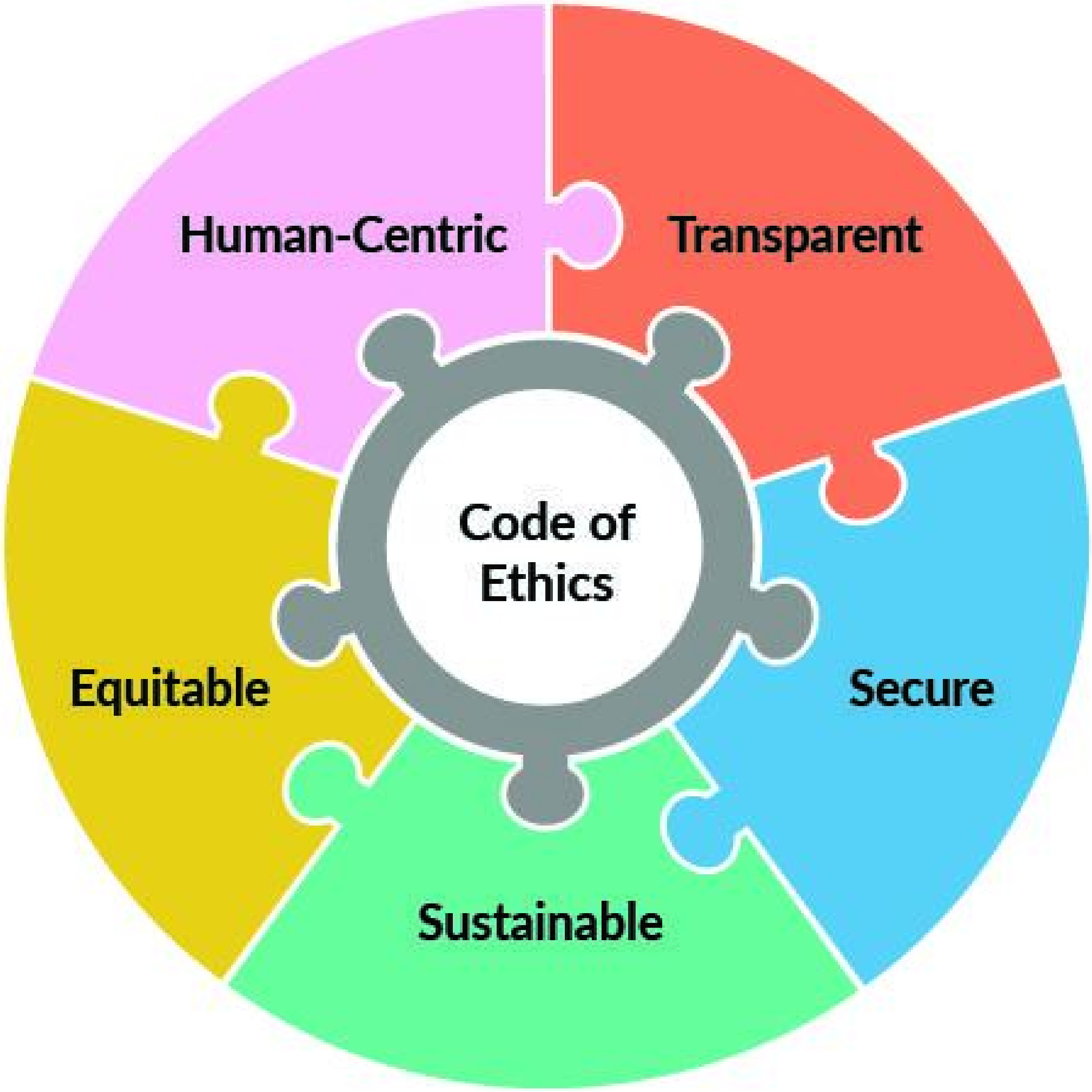
Value #4: Secure

We are stewards of our resident's digital assets and will vigilantly protect the sensitive data entrusted to us (PII, HIPAA, PCI).

Value #5: Sustainable

Technology systems impact our environment. We prioritize technology that reduces environmental waste and is readily sustainable in the long-term.

Digital Values are Foundational to Our Code of Ethics



OUR DIGITAL PRINCIPLES

"Tweet others the way you want to be tweeted."
-Germany Kent, L.A. Journalist & Social Media Expert

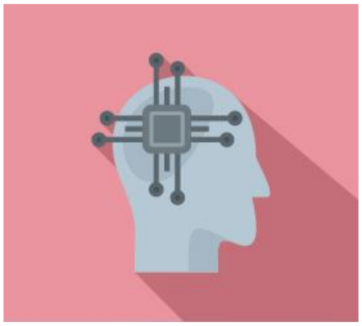
More than just values and guiding principles, this Digital Code of Ethics is designed to be a practical guide for City of Los Angeles departments. Building on our five foundational values, the City of Los Angeles technology leaders have identified and agreed on the digital standards below to ensure that our technology meets both the innovation and ethical expectations of the public:

#1	**WE STRIVE FOR ETHICAL, NOT JUST INNOVATIVE TECHNOLOGY** While innovative features are important, we also take responsibility in foreseeing ethical problems that could overshadow our great features. (HUMAN-CENTRIC, TRANSPARENT, SECURE)
#2	**OUR TECHNOLOGY MUST BE BOTH FUNCTIONAL AND EASY TO USE** We value both what a technology can do for the public and how easy it is to use by the public ("user experience"). Ease of use is a core value for our digital services. This includes access to online, phone, or in-person user assistance when needed. (HUMAN-CENTRIC, EQUITABLE, SUSTAINABLE)
#3	**TECHNOLOGY MUST ENABLE TRANSPARENT GOVERNMENT** Technology provides an opportunity for 4 million busy Angelenos to learn about and get necessary government services. We believe technology should provide insight and access to the government. (EQUITABLE, TRANSPARENT)
#4	**TECHNOLOGY MUST INCREASE ACCESSIBILITY FOR L.A. COMMUNITIES** Websites, apps, and digital portals provide unprecedented access to government services. Our technology is built with all of our communities in mind, regardless of race, disability, language, gender, neighborhood, education level, device, etc. (HUMAN-CENTRIC, TRANSPARENT)
#5	**TECHNOLOGY MUST BE BUILT FOR THE PRESENT & THE FUTURE** We make technology investments that are proven, cost effective, scalable for future demand, sustainable, and based on a competitive purchasing process. (SECURE, SUSTAINABLE)

#6	**WE DO NOT SELL PERSONAL DATA** The data we gather is for the purpose of improving our public services. The City of LA and its vendors will not sell personal data without consent. As digital stewards, we will also secure data according to our Information Security Policy. (HUMAN-CENTRIC, SECURE)
#7	**YOUR LOCATION IS FUNDAMENTAL TO YOUR PRIVACY** The records of where someone has been is fundamental to their privacy. Location data is secured and anonymized, whenever feasible. (EQUITABLE, TRANSPARENT, SECURE)
#8	**OUR TECHNOLOGY RESPECTS USER PRIVACY** The apps, websites, and portals that we provide to the public will not be instruments for unauthorized surveillance. (TRANSPARENT, SECURE)
#9	**WE SEEK TO HIRE A TECHNOLOGY WORKFORCE AS DIVERSE AS L.A.** We believe one of the best methods to prevent racial, gender, and neighborhood bias in our technology is to have a diverse technology workforce. We actively recruit a diverse workforce within the limits of existing human resource laws. (HUMAN-CENTRIC, EQUITABLE)
#10	**WE INVEST IN OUR COMMUNITIES TO REDUCE THE DIGITAL DIVIDE** All Angelenos need the skills and tools to compete in the digital economy, including access to the Internet, digital literacy training, and access to computing devices. (HUMAN-CENTRIC, EQUITABLE)

Artificial Intelligence & Generative A.I.

What is Artificial Intelligence and Generative Artificial Intelligence?



Artificial Intelligence (A.I.) is the science of making things "smart". While the theory behind A.I.-based approaches has existed for decades, its application and use has become much more accessible with the availability of computing and data management at a large scale. Apple Siri and Google Home use A.I. to understand speech, identify what you are asking for, and then provide you with a response. Pandora uses A.I. to propose additional songs you may like based on listening patterns and Google Nest uses A.I. to examine your patterns to adjust your thermostat and turn on/off your smart devices. Generative A.I., such as ChatGPT or Google Gemini, even creates new text, images, audio, and video in a way that seeks to match the work of human beings. A.I. is increasingly used for government solutions, from leveraging A.I.-enabled computer vision to fill potholes on streets to making government information more accessible to non-English speakers. But, while a potentially transformational tool, there are definitely pitfalls with this technology that must be addressed and safeguarded against by the City of Los Angeles to ensure positive benefits for the public.

Dilemmas with Using Artificial Intelligence (A.I.) & ChatGPT

Harnessed appropriately, A.I. can deliver great benefits for governments and society. But, there are important ethical dilemmas and issues to accommodate. As a discipline of computer science, A.I. development must follow responsible best practices for software and IT systems. A.I. can pose special challenges and requires that special attention be paid to: 1) bias 2) transparency 3) misrepresentation.

Bias: Though tempting to think of computer algorithms as objective, A.I. models are susceptible to unfair biases implicit in the data and/or design choices made by the humans that build them. Because humans are ultimately responsible for finding, organizing, and labeling that data, there are multiple ways in which bias can be introduced into the A.I. model. For example, historical volumes of text—often used to train machine learning models that deal with natural language processing or translation—can perpetuate harmful stereotypes if left uncorrected. Seminal work by Bolukbasi et al (https://papers.nips.cc/paper/6228-man-is-to-computer-programmer-as-woman-is-to-homemaker-debiasing-word-embeddings.pdf) demonstrated how easily statistical language models can "learn" outdated assumptions about gender, such as "doctor" being "male" and "nurse" being “female.” Of course, if the City of Los Angeles used a chatbot running on A.I. that communicated to the public based on these outdated assumptions, it would lead to public offense, reduce accessibility, and harm the City’s digital trust. Similar issues, known as embedded biases, have been demonstrated with respect to race as well, which would be unacceptable if part of a City service (https://researchportal.bath.ac.uk/en/publications/semantics-derived-automatically-from- language-corpora-necessarily).

Additionally, beyond forms of bias that can creep into the development of a model, there are also potential biases that arise from how end users interact with a model. Automation bias, for example, is a tendency to favor results of automated systems over human judgment, which can lead to overreliance and misuse of an A.I. system. It’s essential therefore to consider how the outputs of A.I. models are presented and understood within the City of L.A. processes and decisions, in addition to how underlying models are trained.

Transparency: When used by governments, A.I. tools and interactions must be readily explainable for transparency. Explainability is the concept that A.I. systems can be explained by the humans that use them. Explainability is essential to understand and trust the outputs of A.I. systems. These issues apply to humans as well as A.I. systems since it is not always easy for a person to provide a satisfactory explanation of their own decisions. For example, it can be difficult for an oncologist to quantify all the reasons why they think a patient’s cancer may have recurred—they may have an intuition, leading them to order follow-up tests for more definitive results. In contrast, an A.I. system can list a variety of information that went into its prediction: biomarker levels and corresponding scans from 100 different patients over the past 10 years, but have a hard time communicating how it combined all that data to produce a specific prediction. While the logic of traditional software can be laid bare with a line-by-line examination of the source code, a neural network is a dense web of connections shaped by exposure to thousands or even millions of training examples, therefore explainability must be treated specially in the development and use of A.I. tools.

Misrepresentation: Humans make the understandable connection that when they are communicating with someone, they are communicating with another human. Generative A.I., such as Google Gemini, at the City of Los Angeles must be clearly identified as “non-human”, must clearly acknowledge its limitations, and provide an opportunity for a resident to bypass the A.I. tool with an avenue to connect with a real human being. For additional details on this topic, please see Digital Assistants & Chatbots section below.

City Guidelines for Artificial Intelligence & Generative A.I.

For the City of Los Angeles, Artificial Intelligence & Generative A.I. offers transformational opportunities to improve our services and better engage our residents and businesses. The following are key guidelines that address the above dilemmas of bias, transparency, and misrepresentation in the use of Artificial Intelligence:

1. **Do not manage City service delivery using A.I. tools without clear explainability of model/outcomes (TRANSPARENT)**. Whether human oversight or clear explainability, City services must not be allocated or managed by “black box A.I.”.

2. **Do not enter sensitive City or resident data into a public A.I. tool (HUMAN-CENTRIC)**. A.I. tools, such as ChatGTP, track the queries entered into the tool. Do not enter or request the public to enter sensitive data into these insecure tools.

3. **Train A.I. models using concrete goals for fairness and inclusion of diverse communities (HUMAN-CENTRIC)**. Consider the views and types of data represented and what outcomes this application will generate for different users and communities.

4. **Use representative datasets to train and test models (EQUITABLE)**. Assess fairness in datasets, such as identifying representation and discriminatory correlations between features, labels, and groups. Visualization, clustering, and annotations help.

5. **Check new A.I. systems for unfair biases (EQUITABLE)**. Organize a pool of trusted, diverse testers who can adversarially test the system, and incorporate a variety of adversarial inputs into tests to see who may experience unexpected adverse impacts.

6. **Plan out how to ensure explainability before, during, and after the design and training of an A.I. model (SUSTAINABLE)**. Determine the degree of explainability a system needs and understand the behavior and results.

7. **Design the A.I. model to be explainable (TRANSPARENT)**. Use the smallest set of inputs necessary and simplest model possible to meet your performance goals.

8. **Choose metrics to reflect the end-goal and the end-task (SUSTAINABLE)**. Metrics should address the particular benefits and risks of an application. For example, a fire alarm system would need to have high recall, even if it means occasional false alarm.

9. **Communicate explanations to model users and do not train public A.I. tools with sensitive resident data (TRANSPARENT)**. Sensitive data must not be used to train public A.I. tools. Also, “model cards” can be used to explain essential facts to users.

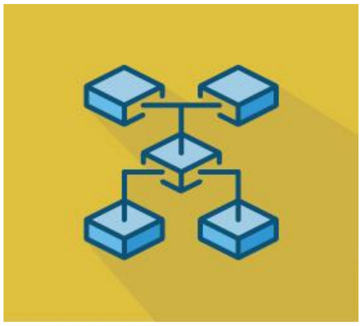
10. **Test repeatedly and follow software engineering best testing practices (EQUITABLE)**. Conduct rigorous testing to incorporate a diverse set of users’ needs.

11. **Disclose to the public when they are using an A.I. tool and provide opportunities to bypass A.I. tool and access a real human being (TRANSPARENT)**.

The Artificial Intelligence & Generative A.I. (ChatGPT) topic above was prepared by the City of Los Angeles Information Technology Agency in collaboration with Chris Hein, Head of Customer Engineering for Public Sector at Google, where his goal is to help public sector organizations become more effective in furthering their mission using technology.

Blockchain

What is Blockchain?



Blockchain technology provides a distributed ledger that presents users with an immutable and consistently-ordered version of data in the form of digitally signed transactions. Blockchain-based distributed ledgers can enable ecosystems of organizations to share in the communication, storage, and processing of data in a decentralized yet trustworthy manner. The decentralized model allows for all of the nodes (computers) on the network to contain the complete ledger of transactions. The result of decentralization is that the unauthorized modification of data stored on the blockchain is virtually impossible. It is for this reason that blockchain can be extremely useful for functions such as voting and financial transactions. Bitcoin is a cryptocurrency with no central bank, but uses decentralized blockchain technology to account for money transfers and payments. Spotify uses blockchain to correlate music artists with their songs and licensing agreements. De Beers uses blockchain to securely and independently track diamonds from mine to jeweler (to reduce fraudulent sales of conflict diamonds). Though originally designed for cryptocurrencies and banking applications, the uses of distributed ledger technology are much broader, encompassing use cases such as property ownership records (home deeds), transparency of government actions, decentralized identity management (digitally confirming you are who say), and tracking of goods (supply chain).

Dilemmas with Using Blockchain

When using blockchain, special attention must be paid to dilemmas that can arise from: 1) using it without a compelling reason (relevance), 2) using features not technologically mature, 3) not properly securing the blockchain platform, 4) excessive energy consumption, 5) exposing confidential data, and/or 6) incorrectness of data.

Not Establishing Relevance: Blockchain is not always the solution to every problem involving data storage and sharing. Consider evaluating alternative technologies and establish a clear justification for using blockchain.

Lack of Maturity: As the underlying technology is still maturing, early blockchain adopters run the risk of being locked into systems that are hard to scale or upgrade. Proper testing and adoption of more mature features and capabilities to mitigate this risk is needed.

Securing Trust: The underlying distributed platform must be as secure as possible, particularly with respect to the parties involved in maintaining and validating the ledger.

Environmental Impact: Proof of Work, used in early protocols, can incur high energy costs.

Maintaining Confidentiality: Confidential, privacy-sensitive data should not be exposed on a ledger. This should be clearly evaluated and mitigated during design and testing.

Guaranteeing Correctness: While blockchain technologies can ensure that data in the ledger is immutable, they cannot always guarantee the correctness of the data. Other application controls must be in place to guarantee the correctness of data.

City Guidelines for Blockchain

For the City of Los Angeles, blockchain affords a unique opportunity to transform government processes with transparency, privacy, and accuracy. The following are key guidelines that address the six dilemmas above in the use of blockchain:

1. **Examine alternatives before using blockchain (HUMAN-CENTRIC)**. Carefully compare blockchain with alternative, even centralized, technology solutions to see if it is truly a good fit for users and the problem trying to be addressed.

2. **Be honest and accommodate for current technology limitations (SUSTAINABLE)**. Seek solutions based on open and common standards that are easy to upgrade and scale over time as the technology matures; avoid vendor lock-in.

3. **Thoroughly plan for both current and expanded blockchain decision-making (SUSTAINABLE)**. Adopt governance that includes how validators are chosen, how users are authorized for their roles, and how open it is.

4. **Consider environmental impact and carbon offsets if selecting blockchain solutions (SUSTAINABLE)**.

5. **Protect confidential data (SECURE).** Have a clear policy about what data is entered on a public ledger; ensure confidential data is suitably encrypted. Ensure that private keys are kept secure.

6. **Implement policies and system controls to ensure that data entered on a blockchain ledger is truthful and correct (SECURE)**.

The Blockchain topic above was prepared by the City of Los Angeles Information Technology Agency in collaboration with Bhaskar Krishnamachari, Professor of Electrical and Computer Engineering at the University of Southern California. Professor Krishnamachari has co-authored more than 300 articles and 3 books focused on wireless networks, the internet of things, and distributed systems. He is a recipient of the National Science Foundation CAREER award, the ASEE Terman Award, and has been featured on MIT Technology Review's TR35 list, as well as Popular Science's “Brilliant 10”.

Data & Predictive Analytics

What is Data Analytics?

Data analytics is the science of analyzing data to understand trends and patterns. Predictive analytics is a specialized form of analytics that assesses current and historical trends to make predictions about future events. Netflix uses data analysis to write algorithms that suggest movies for you to watch based on your past watch history. Major League Baseball uses data analytics to evaluate player performance and recruit new talent as evidenced in the movie *Moneyball*. Data analytics at the City of Los Angeles departments is the examination of data to understand the impacts of City services, departmental programs, or public policy. While data analytics is a crucial element of becoming a "data driven government", it can also be misused, resulting in unintended negative consequences for L.A.'s communities.

Data analytics can be performed in two forms. First, a "report" based on longitudinal data across a period of time. A report represents findings regarding what has happened and often includes recommendations for changes to policies or systems. Second, a "dashboard" delivered in real-time, providing automated decision making systems (ADS). Both types of data analysis require careful thought, attention to detail, and a reliance on the City's ethical values to bring useful conclusions.

Dilemmas with Data Analytics Projects

For data analytics, special attention must be paid to: 1) data issues and 2) analysis issues.

Data Issues: All data has bias. Data from City systems inherently contain novel biases. By acting as a "digital exhaust" of city administrative programs, the data automatically encodes a bias from the city program itself. To ensure ethical and accurate results, data analysts must identify and quantify how the data is biased, avoiding statements like "the data says x". Data can also contain implicit bias (attitudes that affect us unconsciously). For example, 311 graffiti complaints could be a misrepresentation of actual graffiti across Los Angeles as some communities use 311 to report graffiti much more than others.

Analysis Issues: When making policy recommendations, bias must be presented properly to decision makers (i. e. these results skew this direction and here's why). Secondly, data scientists must not yield to the pressure to make results conform to an expected result. Thirdly, limits of the analysis must be clearly communicated. As Danah Boyd writes in *Engaging the Ethics of Data Science in Practice,* "*Technical actors are often far more sophisticated than critics at understanding the limits of their analysis. "* Stakeholders should be informed of the hard earned context learned by the data analyst during the analysis. Fourth, departments must be able to audit and explain dashboards and

Automated Decision Making Systems (ADS). An automated result must have underlying knowledge of how it is derived, used, and what biases may exist. Fifth, visualizations can unintentionally misrepresent results. Data visualizations must abide by common standards.

City Guidelines for Data Analysis

As L.A.'s elected leaders increasingly rely on "data driven" government to inform policies, ethical and accurate data analysis is of premium importance. The following are key guidelines that address the above dilemmas with data and analysis issues in the use of data analysis:

1. **Data analysis projects must be reproducible and traceable from data to conclusion (TRANSPARENT)**. Famous "Excel Error that Changed the World" was discovered by UMass students trying to reproduce Harvard economists' results.

2. **Data analysis results must be anonymized and aggregated to protect privacy (SECURE)**. However, aggregation must not hide critical insight into potential racial or demographical impacts.

3. **Data must be stored with least privilege access by data analysts (SECURE)**.

4. **Data analysts must not use data for purposes other than what was authorized by the data provider or attempt reidentification (SECURE).**

5. **Automated Decision Making Systems and dashboards must be interpretable (TRANSPARENT)**. Inputs and outputs must be documented with understanding of how data is transformed, used, and known influences on the model (no "black boxes").

6. **Avoid using ZIP codes/ZCTAs as unit of aggregation (HUMAN-CENTRIC)**. Census tracts or LA Neighborhoods are often more relevant for reporting results.

7. **Results must be auditable (TRANSPARENT)**. While some datasets must be private, reports, analysis, and code should be open for inspection and questions.

The Data Analysis Standards above were prepared by Hunter Owens, former Technical Lead of the Data Science & Predictive Analytics Team at the City of Los Angeles Information Technology Agency. Before working for the City of L.A., Hunter worked at Obama for America and the Center for Data Science & Public Policy.

Digital Assistants & Chatbots

What are Digital Assistants & Chatbots?

Digital assistants and chatbots ("bots") are software that understands natural language voice commands and provides information or completes tasks for the user. Common examples are Microsoft Cortana, Amazon Alexa, Apple Siri, and Google Home. These digital assistants can take dictation, read messages aloud, setup appointments, schedule meetings, set reminders, and more. Powered by conversational artificial intelligence (A.I.), these tools are increasingly used by companies to offer new services to customers, reduce call hold times, and expand service hours. At the City of Los Angeles, our Chip the Chatbot has *answered over 300,000 resident questions* through LACity.gov, the LABAVN.gov business portal, LAPD Recruitment, and other websites. While automated digital assistants can improve equitable access to City services and customer service, they also have the potential to undermine public trust and negatively affect our residents.

Dilemmas with Using Digital Assistants & Chatbots

In order for Los Angeles residents and businesses to benefit from the City of Los Angeles' digital assistants and chatbots, we must ensure we address the dilemmas that can arise from: 1) not properly identifying themselves as a bot 2) being unknowledgeable or unreliable 3) showing cultural bias or disrespect.

Bots Misrepresenting Themselves: Humans make the understandable connection that when they are communicating with someone, they are communicating with another human. The technological development of digital assistants and chatbots can pose a sociological challenge when the human observes too many commonalities between the bot and another human (aka the "uncanny valley"). This is readily addressed by the bot clearly identifying itself as a technology tool for human assistance and not as another person.

Bots That Are Unknowledgeable or Unreliable: We've all experienced the frustration of a phone tree that makes it impossible to get to a person who can help us or answer our question. A bot that cannot answer your questions conveys the same frustrating feeling. Bots need to be pre-loaded with a substantial amount of answers BEFORE being made available to the public. Secondly, a knowledgeable bot will be frustrating if answers are unpredictable or unreliable. A well trained digital assistant must consistently answer questions from the public.

Bots That Are Disrespectful of Racial or Cultural Differences: As bots often have human-like personas, it is especially important that they interact respectfully and safely with the public. The possibility that A.I.-based systems can perpetuate existing societal biases, or introduce new biases, is a top concern in the scientific community. Bots must include cultural considerations, built-in safeguards, and protocols to handle the diversity of our community.

City Guidelines for Digital Assistants & Chatbots

At the City of Los Angeles, digital assistants and chatbots offer the promise of improved customer service options for L.A.'s residents, businesses, and visitors. The following are key guidelines to address the above dilemmas in the use of digital assistants and chatbots:

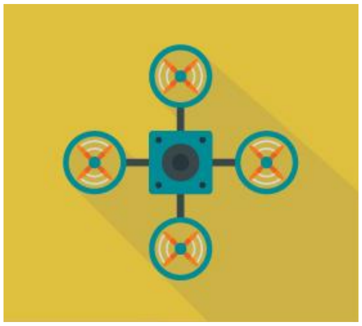
1. **Before developing a digital assistant or chatbot, clearly define its purpose, target audience, and value it will bring (HUMAN-CENTRIC)**. Understanding this mission is essential during the design, build, and maintenance of the bot.
2. **Be fully transparent to the public that they are using a bot and acknowledge any limitations (TRANSPARENT)**. This builds public trust.
3. **When initiating the conversation with a bot, be sure to clearly establish how the bot can help and any limitations up front (TRANSPARENT).**
4. **Ensure bots comply with ADA 508 accessibility standards (EQUITABLE).**
5. **To avoid offensive speech, program your bot to ensure it limits the "surface area" for norms violations (HUMAN-CENTRIC)**. For example, a bot whose purpose is to answer business permitting questions should never engage on topics of race, gender, religion, etc. If necessary, deploy a two-way filtering mechanism with a customizable threshold of tolerance to control what your bot takes in from users and says in response to prevent malicious users from re-training your bot.
6. **Ensure diversity in your bot development team (EQUITABLE)**. A diverse development team is a key step in ensuring the bot addresses cultural differences.
7. **Systematically assess data used for bot training (EQUITABLE)**. Assess bot training data to ensure it has appropriate representativeness and quality, taking steps to understand the lineage and relevant attributes of training data. Consider the use of bias detection tools to ensure your bot treats all people fairly.
8. **Provide opportunities for the user to bypass the digital assistant and access a real human being (HUMAN-CENTRIC)**. Respect a user's preferences.
9. **Periodically review analytics about bot accuracy and reliability (SUSTAINABLE)**. If bot accuracy is less than 51%, take steps to improve or else remove bot from public use. Sentiment analysis tools are also valuable.

The Digital Assistant & Chatbot Standards above were prepared by the City of Los Angeles Information Technology Agency in collaboration with Microsoft Corporation through the writings of Lili Cheng, Corporate Vice President and Distinguished Engineer. Lili manages the Microsoft A.I. and Research division, responsible for the Microsoft A.I. developer platform.

Drones & Remotely Piloted Aircraft

What are Drones & Remotely Piloted Aircraft?

A drone or remotely piloted aircraft is a small, flying robotic device that is remotely controlled by a human operator or flies autonomously through software-controlled flight plans using embedded computer systems, onboard sensors, and GPS. Most of us have observed a hobbyist flying a remote controlled drone at the park or beach. Filmmakers have used quad copters (four propellers) with cameras to get exciting aerial shots for movies. Companies, like Amazon, have been testing the use of large flying drones to deliver packages to customers. While remote controlled aircraft are nothing new, drones have become much more sophisticated in their capabilities (software-controlled flight, cameras, GPS, battery power, and relatively low cost). Drones are becoming powerful tools for getting situational awareness or replacing humans for dirty or dangerous jobs. Increasingly, drones are being used at the City of Los Angeles for firefighting, search and rescue, and utility inspection. However, automated aerial vehicles can raise ethical concerns about the data that drones can obtain and store. As drones are under the control and influence of the humans that use them, our Digital Code of Ethics includes potential ethical dilemmas and the guidelines we apply to address them.



Dilemmas with Using Drones

When using drones, special attention must be paid to dilemmas that can arise from: 1) using drones only for unauthorized and unethical purposes 2) conflicts with other aircraft 3) insecure data collection and storage of images or video.

Using Drones For Unethical Purposes: The average resident feels an invasion of privacy when a drone hovers above their home, regardless of whether it is owned by another resident or the government. California State law (AB 856 // 2015) prohibits “entering the airspace of an individual in order to capture an image or recording of that individual engaging in a private, personal or familial activity without permission.” While there is a compelling commercial usage for drones at the City of Los Angeles, video and images must never be collected or stored of individuals engaging in a private, personal, or family activity at their home.

Conflicts with Other Aircraft: Drones are not the only things in the sky. One major issue has been the use of drones in conflict with pilots of aircraft in occupied airspace. In Washington for example, a news helicopter was covering a fire when a drone started flying a few feet away from the helicopter. The FAA now receives over 100 complaints per month. It is critical for the City of Los Angeles drone usage to abide by existing laws as it relates to uncontrolled airspace (Class G) and controlled airspaces.

Insecure Storage of Drone Data and Video: Drones provide a unique vantage point and often capture sensitive video and images. If a drone gathers data for its commercial purpose, then it must be securely captured and stored by the City department using the drone in compliance with the City of Los Angeles Information Security Policy.

City Guidelines for Using Drones

For the City of Los Angeles, drones are an effective way to coordinate resources for public safety (e.g. fighting a fire) and to perform dirty or dangerous work instead of a human. The following are key guidelines that address the above dilemmas in the use of drones.

1. **Use of drones must first be approved by the City of Los Angeles City Attorney's Office to ensure adherence to current laws (HUMAN-CENTRIC)**. Requests must detail scope, justification, and data protection assessment (describe collection, use, and deletion of personally identifiable data).
2. **Ensure ethical drone purposes before buying one (HUMAN-CENTRIC)**. Before acquiring a drone, establish compelling purposes that don't violate State or Federal law. Ensure these purposes are clearly understood and adhered to by drone pilots.
3. **Train drone pilots and maintain equipment (SUSTAINABLE)**. Establish proper training curriculum for pilots and maintenance regimen for all drones to prevent drone failure in which injury or damage can result.
4. **Perform required FAA registration and apply drone markings (SUSTAINABLE)**.
5. **Abide by FAA airspace regulations**. Be sure to abide by all FAA drone airspace regulations and gain authorizations when required (e.g. below 400 feet in uncontrolled Class G airspace).
6. **Keep drones within visual line of sight per FAA application of Part 107 (SECURE)**
7. **Delete footage resulting from unlawful operations immediately (HUMAN-CENTRIC)**. If footage of residents is obtained by a City of Los Angeles drone through unlawful operation it must be deleted.
8. **Drones must be secured from hacking (SECURE)**. Ensure the drone has encrypted communications, default passwords are changed to long passwords, and chain of custody is established to ensure sensitive drone data is stored securely. This is necessary to avoid "maldrone" hacking attempts or data breaches.

The Drone and Remotely Piloted Aircraft topic above was prepared by Ted Ross, CIO of the City of Los Angeles and General Manager of the Information Technology Agency (ITA). Ted has over 24 years of private and public sector technology experience, has been featured in Fortune Magazine, The Wall Street Journal, and The Economist, and has earned various awards, including Top 25 Doer & Dreamer and CIO of the Year according to LA Business Journal.

Facial Recognition

What is Facial Recognition Technology?

Facial recognition technology is the software and systems used to detect, analyze and compare facial features in order to identify unique individuals. Most of us have used facial recognition technology to unlock our Apple or Android smartphone by simply looking at the screen. Facebook and Google use facial recognition to identify and tag people in your photos, so you can easily search for photos of your friends. At the City of Los Angeles, any usage of facial recognition raises serious concerns around privacy and racial profiling, requiring approval by the Office of the City Attorney. This technology has become viable as the quality of facial recognition results has evolved over the past 60 years through the use of increasingly sophisticated statistical models supported by machine learning which have proven to outperform human facial recognition in certain cases. Technology even allows mobile face recognition through drones and smart glasses. At this time, performance is imperfect, proving to be variable and potentially prone to error or bias.

Dilemmas with Using Facial Recognition Technology

For facial recognition, special attention must be paid to dilemmas that can arise from: 1) the way the technology is deployed and 2) inherent system features.

Deployment Issues: Facial recognition databases contain personally identifiable information (PII) about individuals. For acceptable usage, this information is sensitive and must be secured against data leakage or unauthorized access. Secondly, facial recognition is often cross-referenced with known “watchlist” databases that may be erroneous themselves, resulting in misidentification. Third, some facial recognition systems tend to discriminate based on classes like race and gender. The globally-recognized National Institute of Standards (NIST) conducted studies in 2019 and found empirical evidence that Asian and African-Americans were up to 100 times more likely to be misidentified than Causasian subjects, with Native Americans having the highest false positive rate of all ethnicities.

Fourth, facial recognition may indiscriminately identify children (minors) and vulnerable individuals and store data about them and, by default, their movements. The collection of this data may be highly inappropriate and unjustified. Fifth, regulations governing the use of facial recognition are rapidly evolving. Even a justifiable and ethical usage of facial recognition must adhere to federal, state, and local ordinances.

System Feature Issues: Model performance is dependent upon the quality and quantity of training data. If training data is not representative of the population, it will skew results and generate false matches, especially for particular ethnicities, and may not be able to handle occlusion adequately. Secondly, all systems are prone to error, especially as lighting conditions, movement, distance from the subject, and occlusion erode performance. The risks of mis-identification must be accounted for and accommodated with any facial recognition system.

City Guidelines for Facial Recognition Technology

At the City of Los Angeles, the usage of facial recognition is subject to privacy considerations and protections against racial profiling, requiring an extremely compelling justification and greater safeguards than other emerging technologies in these standards. The following guidelines address the above dilemmas in the use of facial recognition:

1. **Use of facial recognition must first be approved by the City of Los Angeles City Attorney's Office to ensure adherence to current laws (HUMAN-CENTRIC).** Requests must detail scope, justification, and data protection assessment (describe collection, use, and deletion of personally identifiable data).
2. **Facial recognition systems must be thoroughly tested (HUMAN-CENTRIC)**. Tests must involve real world conditions with the results evaluated against expected performance industry reports, NIST evaluations, etc).
3. **Facial recognition systems must be evaluated for the specific, authorized usage (HUMAN-CENTRIC)**. Systems on the market can exhibit performance idiosyncrasies with differing strengths and weaknesses that must be accounted for.
4. **Before soliciting for a facial recognition system, specific use case requirements must be detailed and the product must meet those requirements (HUMAN-CENTRIC)**.
5. **Alternative biometric or traditional solutions must be considered first (HUMAN-CENTRIC)**. Facial recognition may not be necessary for desired outcome.
6. **Facial recognition systems should be clearly identified via signage and other public notifications using conditions of entry, terms of employment, etc (TRANSPARENT)**.
7. **Facial recognition systems must be audited every two years (SUSTAINABLE)**. This is necessary to confirm proper collection, prevent expanded scope, maintain accuracy across races, deletion of PII, data security, safeguards for minors, etc.
8. **Facial recognition system must adhere to L.A. Info. Security Policy (SECURE)**.
9. **Facial recognition data should be retained only as long as it's necessary for legitimate purposes and then destroyed (SECURE).**

The Facial Recognition Standards above were prepared by the City of Los Angeles Information Technology Agency in collaboration with Nick Ingelbrecht, Senior Research Director with Gartner Inc.

Healthcare Data

What is Healthcare Data?

Healthcare data is information and data which relate to the physical/mental health of an individual or the provision of health services to that individual. This data includes your blood type, existing medical conditions, medical procedures you have had, medications you are using, blood pressure, etc. Healthcare data is a very sensitive form of personally identifiable information (PII), which is information that permits the identity of an individual to be reasonably inferred. If maliciously or accidentally revealed, health data can result in various harmful actions, such as embarrassment, discrimination, impersonation, and even blackmail. While some City of Los Angeles departments (e.g. L.A. Fire Department paramedics) have specific needs to gather healthcare data, other City departments must avoid gathering and storing this information. Under the Health Insurance Portability and Accountability Act (HIPAA), health information is privileged and cannot be shared without consent, unless for the safety and welfare of others.

Anonymized healthcare data can be beneficially used in biomedical and health research for preventive, diagnostic and therapeutic public benefits. At the City of Los Angeles, analysis of employee health data has revealed workplace safety issues that were resolved for the safety of employees. Anonymized resident health data has been used by universities to reveal public health issues, environmental hazards, and influence urban plans. However, there are many serious potential issues that must be addressed.

Dilemmas with Storing Healthcare Data

When storing health data, special attention must be paid to dilemmas that arise from 1) limits of de-identification 2) added pressures on consent procedures 3) transferability of health data to other domains 4) risks associated with analytics 5) meaningfulness of consent:

Limits of De-Identification: Healthcare data may be re-identifiable, even when substantial identifiable information has been removed. This may result in insufficient privacy protection for individuals in the data set. New opportunities for data linkage and the integration of different data sets (e.g. social networking, internet searches, web postings, medical devices, wearables, or smartphone apps) can make re-identification possible.

Added Pressures on Consent Procedures: When data is collected and stored for future use, it is difficult to anticipate future uses and therefore difficult to ensure fully informed and specific consent from the individual. Secondary and subsequent data use should be more transparent, and allow people to consent (or withdraw consent) for both anticipated and unanticipated future uses.

Transferability of Healthcare Data to Other Domains (and Vice Versa): Data sets can be used to make health-relevant inferences pertaining to individuals. Thus, data that was not collected for health-relevant purposes can unethically be used in a health-relevant way.

Risks Associated With Predictive Analytics & Inferences: Individuals don't have insight on how their own data is used to make inferences or predictions about them. If there is a negative impact to them, even if inaccurate data is used, there are no easy options available to them to rectify the harm/error or seek redress.

Meaningfulness of Consent When Required for Services: Consent, authorization, or permission for data release is less meaningful when patients have little choice — such as emergency ambulance services, mandatory health insurance, drug prescription subsidies, or use of health-related social networks, smartphone apps, wearables, and monitors.

City Guidelines for Healthcare Data

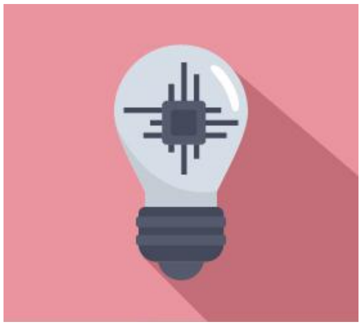
For the City of Los Angeles, healthcare data is essential for some services (e.g. ambulances) and beneficial for identifying public health issues. The following are key guidelines that address the above dilemmas in the storage and use of Healthcare Data:

1. **Do not gather or store L.A. resident healthcare data, unless essential to your department's responsibilities, e.g. LA Fire Department (HUMAN-CENTRIC)**.
2. **Respect the obligation to protect an individual's privacy (SECURE)**. Understand the rules and laws regarding healthcare data and Protected Health Information (PHI).
3. **Store the minimum personal data needed to achieve outcomes (SUSTAINABLE)**.
4. **Except in a medical emergency, allow individuals the opportunity to determine how their personal data may be used or shared (TRANSPARENT)**. This should include providing consent and methods to control use/access to their data.
5. **Always use data for the purpose which it was collected/consented for (SECURE)**.
6. **Do not share healthcare data with other agencies, unless understood and consented to by the individual (TRANSPARENT)**. Then, anonymize and restrict access to the shared data using the City of Los Angeles Data Sharing Agreement.

The Healthcare Data topic above was prepared by Timothy Lee, Chief Information Security Officer, and Madeline Dia, Information Security Governance Manager, at the City of Los Angeles Information Technology Agency. Tim and Madeline bring over 40 years of combined experience in data security and technology management.

Internet of Things (IoT) & Sensors

What is the Internet of Things (IoT)?



According to Oxford Dictionary, the Internet of Things (IoT) is “the interconnection, via the Internet, of computing devices that are embedded in everyday objects, enabling them to send and receive data.” While not one specific device or technology, the Internet of Things (aka the Internet of Everything) is the digital connection between electronic devices (computers, sensors, cameras, smartphones, home appliances, and other networked devices) that enables tremendous new capabilities between internet-connected devices and the humans around them. This includes “smart” light bulbs that can be controlled by your smartphone and Fitbit watches that track your daily step count. Ring doorbells that track when a package is delivered and send photos of your visitors are IoT devices. Parking meters that allow use of credit cards and automatically notify the City when they are broken are also IoT devices. These sensors are generating unprecedented amounts of data and posing unprecedented challenges around security, privacy, and sustainability. As of 2024, there are over 19 Billion IoT connected devices, expecting to increase to over 40 Billion devices in the next five years. As the City of Los Angeles increasingly uses sensors and connected devices to improve our urban landscape and gather important information about water usage, traffic, pollution, and noise, the ethics around IoT becomes an important set of guidelines.

Dilemmas with Using the Internet of Things (IoT)

When implementing and using IoT sensors, special attention must be paid to dilemmas that arise from: 1) physical safety; 2) informed consent; 3) privacy; 4) information and device security; 5) congestion of IoT devices.

Physical Safety: IoT allows for increased automation and “action-at-a-distance”, allowing the digital world to affect the physical one. For example, an IoT connected automobile is able to identify that the owner is approaching the vehicle, sense the temperature, turn itself on, and change the thermostat to a cozy 72 degrees. Across a city, you can imagine the tremendous benefits of a living, adjusting “Smart City” that alters traffic and lighting for the benefit of the public. If hacked and maladjusted, this could impact the physical safety of its occupants, so substantial controls are needed to ensure physical safety when using IoT.

Informed Consent: Informed consent is when someone impacted by technology agrees to its use with a clear understanding of the implications and consequences of its use. With an increasing number and integration of public and private IoT devices, it becomes much more difficult to gain informed consent, often devolving into “implied consent”. Getting to informed consent with IoT devices is important in the collection of any personal information.

Privacy: The increasing array of IoT sensors must be careful of the privacy rights of City of Los Angeles residents. First of all, IoT data must abide by the City's privacy standards on what can be collected. For example, noise or pollution monitoring data is acceptable in a neighborhood, while audio recordings of a resident is not. Secondly, IoT data must not invade privacy in how the data is used. For example, a well known merchandising store analyzed and profiled client purchasing habits and inappropriately sent a pregnancy related mailer to a teenage girl whose family was unaware. The average American viewed this as an invasion of privacy.

Information & Device Security: IoT technology can provide security concerns for three reasons. It can be physically accessible to a hacker. Is often constantly in communication with its network. Finally, it is typically a low cost device that infrequently receives security patches. This requires security of the data collected by the IoT device, the communication channel, and the device itself. These security concerns were demonstrated in 2016 when the Mirai malware controlled a large number of IoT devices and used them to commit a "distributed denial of service (DDoS)" cyber attack. The City of Los Angeles cannot allow government devices to be data breached or converted into a zombie bot that assists in damaging the property of others.

Congestion by IoT Devices: With the proliferation of IoT sensors, City of Los Angeles departments must collaborate to install multi-purpose devices wherever possible to prevent congestion of sensors and devices in the urban landscape. Through appropriate coordination, devices can perform multiple purposes making them easier to secure, more cost effective, and reduce unsightly congestion of digital devices in public.

City Guidelines for IoT & Sensors

For the City of Los Angeles, the Internet of Things provides tremendous benefits for monitoring conditions in our urban landscape (traffic, pollution, public safety, excessive noise, etc) and providing real time feedback/response to improve quality of life for L.A.'s residents. The following are key guidelines that address the above dilemmas in the use of IoT and sensors:

1. **Acquire IoT devices in coordination with other City Departments through the IT Policy Committee (SUSTAINABLE)**. Single purpose IoT devices will be expensive, difficult to secure, and create unsightly congestion in L.A.'s streets. City Departments preparing to implement IoT devices must first communicate and coordinate with other departments using an agenda item in the City's Information Technology Policy Committee (ITPC).

2. **Analyze the type of data you will capture and establish appropriate levels of security using Information Security Policy (SECURE)**. Assess the type of data being collected by the IoT sensor, classify using the City of L.A. Information Security Policy, and institute the appropriate level of security. The following are considerations to secure devices (based on the sensitivity of data collected):
    a. Periodic patching of device operating system and software
    b. Implement encryption at rest and in transit
    c. Place sensors on secure communication networks (e. g. cellular).
    d. Hide and anonymize IoT identifiers. Ensure that IoT sensor identifiers are hidden and anonymized to prevent collection analysis by hackers.
    e. Manage encryption keys to prevent unauthorized decryption of devices.
    f. Secure boot technology to ensure only known software can run on device.
    g. Use of hardware-rooted trust chains to prevent low-level software attacks.
    h. Use software that identifies compromised or malfunctioning devices so they can be repaired or removed.
3. **Establish security for systems that interconnect with your IoT (SECURE)**. An IoT device operates in concert with other connected devices (using an attack vector to compromise the device). Establish a network diagram of interconnected IoT devices with permissions between each other. Implement security for all connected devices at the level required by the most sensitive devices (i.e. secure them all at the level required for the most security sensitive device).
4. **Do not place IoT sensors directly onto the City network (SECURE)**. By nature, IoT is often in the public and potentially accessible by the public. It is forbidden to connect an IoT device directly onto the City of L.A. network, allowing a potential threat vector for hackers to access the internal City network. Connectivity needs to be provided through separate communications vehicle (e.g. ISP, cellular, etc).
5. **Limit access of IoT sensors to the public (SECURE)**. IoT sensors are often in the public domain, which requires efforts to limit physical access using locked cases, elevation on light poles, hiding from sight, etc.
6. **Share data with other City departments and open data portal (TRANSPARENT)**. The City of Los Angeles seeks to make publicly available raw data in easy-to-find and accessible formats…made freely available for use by the public, subject only to valid privacy, confidentiality, security, and other legal restrictions. Unless subject to the exceptions, IoT data needs to be added to the Data. LACity.org open data portal.

The IoT Standards above were prepared by Joyce Edson, retired Executive Officer, of the City of Los Angeles Information Technology Agency. Joyce has over 33 years of enterprise IT and management experience and is a founding member of the Intelligent IoT Integration (I3) consortium with the University of Southern California (USC) and 90 other member organizations.

Social Networks & Social Media

What are Social Networks & Social Media?

More than 5.5 billion people around the world use the Internet, of which, 4 billion people are a part of an online, social network using a social media platform (Pew Research, 2024). More than 72% of Americans use social media (Pew Research, 2024). That is 248 million Americans interacting with each other, with businesses, and with government entities at all levels. Social Media is interactive computer-mediated technologies dedicated to facilitating community-based input, interaction, content-sharing, content-creation, and collaboration. These channels include social networking sites, weblogs (blogs, vlogs, or microblogs), podcasts, online chat sites, and forums. Examples include Instagram, Youtube, Facebook, X, LinkedIn, Snap, and TiKTok. For the City of Los Angeles, social media and social networks can transform the ways in which our government, our City departments, and our elected officials relate to the public. These powerful sets of tools can be highly beneficial by allowing constituents easy, engaging, and immediate access to government information or services. However, as with any publicly shared medium there are risks and ethical issues that must be addressed.

Dilemmas with Using Social Networks & Social Media

When using social media, special attention must be paid to dilemmas that arise from: 1) maintaining transparency; 2) impartiality in messaging and branding; 3) censorship;
4) active engagement with the public; 5) privacy concerns with social media monitoring tools.

<u>Maintaining Transparency</u>: Governments hold positions of power. Access to government is a fundamental right for every L.A. resident. In social media, openness and transparency are driving principles when communicating with the public. Letting residents see and hear an unfiltered side of government service is genuine and typically a best practice approach.

<u>Impartiality in Messaging</u>: Social media coordinators must remain impartial when sharing official messaging and be authentic in representing the brand, voice, and goals of their government organization when communicating with and engaging target audiences (residents, businesses, visitors, and other stakeholders). To be authentic is to be accurate, clear, concise, and responsible in communications, regardless of personal opinions.

<u>Censorship</u>: City employees who coordinate or manage a City social media account are stewards of interactive, public forums. Public forums managed by government and elected

officials are subject to First Amendment civil liberties and may not discriminate against or censor the viewpoints of private speakers.

Active Engagement with Public: By its nature, social media is bi-directional communication that should be engaging. Social media coordinators are tasked with engaging the public, especially during times of emergency, disaster or public health crises.

Privacy Concerns with Social Media Monitoring Tools: Social media monitoring or listening tools analyze public discussions on social media. These tools provide insight into public sentiment, access to real-time feedback, allow timely contribution to open conversations, and provide the ability to respond to public questions. However, while not private, some social media users may be put off by stepping into their conversation. Please consider tone and stakeholder comfort if using a social media monitoring tool to engage the public.

City Guidelines for Social Networking & Social Media

For the City of Los Angeles, social media provides transformational opportunities to listen to and engage the public. The following are key guidelines that address the above dilemmas in the use of social networks and social media:

1. **City social media messages must be on mission, accurate, and respectful (HUMAN-CENTRIC)**. Employees and elected officials are responsible for ensuring social media content is relevant to their organization's mission, professionally presented, accurate, and respectful of L.A.'s diverse communities. Messages with bad grammar or that are unfactual should be removed immediately.

2. **City social media must be unbiased and impartial (TRANSPARENT)**. City social media accounts must remain unbiased about prioritizing one political agenda over another. Messaging should guide residents to engage their elected officials directly.

3. **City social media must understand their department's or elected official's brand (HUMAN-CENTRIC)**. Consistency is important, especially when multiple people manage accounts. Messaging should also be vetted, verified, and credible.

4. **L.A. City government social media platforms must not participate in data surveillance or data sharing with third-parties (SECURE)**.

5. **Use the City of Los Angeles Social Media Policy for guidance (SUSTAINABLE)**. The City policy contains guidance in the use of social media.

The Social Media topic above was prepared by Mariana Ferraro, Social & Digital Media Director at the City of Los Angeles Information Technology Agency. Mariana is an award-winning Television Executive with over 22 years of experience in broadcast production, digital marketing & communications.

Virtual and Augmented Reality

What is Virtual or Augmented Reality?

Virtual reality (VR) is “an artificial environment which is experienced through sensory stimuli (such as sights and sounds) provided by a computer and in which one's actions partially determine what happens in the environment” (Webster’s Dictionary). VR is associated with a headset (Meta, Apple, Microsoft, Goertek, etc) that blocks out the real world around you while substituting it with a computer generated reality that allows for our interaction in one form or another. While commonly associated with the gaming industry, VR has many applications, including at the City of Los Angeles, for promoting tourism, highlighting the L.A. River, and recruitment of potential City employees. While related, Augmented Reality (AR) is “an enhanced version of reality created by the use of technology to overlay digital information on an image of something being viewed through a device (such as a smartphone camera).” While VR is a complete environment that replaces reality, AR only enhances what we see by adding digital elements. One of the most recognizable AR apps was Pokemon Go, which used built-in GPS, camera, and the screen in the smartphone to allow users to digitally catch and train Pokemon characters in real-life locations. At the City of Los Angeles, AR has been used to train employees in complex job tasks (e.g. L.A. Fire Department headset repair) and test technical employees for job aptitude. If you have ever used your computer to imagine what colors or furniture would look best in your home or used your smartphone to see how different clothes would look on you, then you are no stranger to AR.

Dilemmas with Using Virtual Reality (VR) & Augmented Reality (AR)

While virtual and augmented reality can be powerful technologies, special attention must be paid to dilemmas that arise from: 1) safety 2) behavioral manipulation 3) privacy/consent 4) security.

Safety: The physical safety of AR/VR users must be considered. These issues came to the forefront during the popularity of Pokemon Go. Many car accidents, lawsuits, and fatalities were the result of players paying too much attention to their digital environment and not their actual physical one. In addition, these altered states can result in nausea and bouts of dizziness. The overall safety of users must be factored in during the creation process.

Behavioral Manipulation: An immersive environment (VR) or digitally augmented environment can be very suggestive and persuasive, especially among vulnerable groups (children, elderly, those with cognitive disabilities, the mentally ill, etc). City departments must closely review and scrutinize VR/AR content they create to understand how it can affect their users and avoid content that reinforces negative behavior.

Privacy/Consent: An immersive or augmented experience may purposefully or inadvertently gather digital information from its users. Users would need to provide explicit permission before the collection or sharing of information. Additionally, privacy is not just about whether or not information is collected/shared, but about safety. Tracking current and historical locations may enable criminal conduct that puts the safety of users at risk.

Security: The cyber security risks of AR/VR should be considered. Security must be included during the creation of the application. Immersive or augmented environments must be secure and safe from hackers. The physical and mental safety of users is paramount among the concerns that can result from security or data breaches.

City Guidelines for Virtual & Augmented Reality

At the City of Los Angeles, the usage of virtual or augmented reality can be a tremendous benefit to the public so long as safety, behavioral, privacy, and security concerns are considered. The following are key guidelines that address the above dilemmas in the use of virtual and augmented reality:

1. **Warnings and disclaimers must be provided to ensure physical safety when using Virtual or Augmented Reality (HUMAN-CENTRIC)**. Instruct the user to access content in a safe place without distraction or require them to be seated.

2. **Negative behavioral impacts must be assessed and avoided (HUMAN-CENTRIC)**. Creators of AR/VR content must consider and test mental consequences on a focus group prior to public release. Identify the potential risks and symptoms that may arise and make content changes or else eliminate the app.

3. **Avoid data collection or obtain explicit consent from the user if data collection is necessary (TRANSPARENT)**. Ensure that users are aware of the data collected (if any) and who it would be shared with. Users should have an option to opt out of any collection of data, unless for the purpose of job testing.

4. **Apply security to all Virtual and Augmented Reality applications (SECURE)**. Current encryption standards should be built into all AR/VR applications. If data must be collected, it must adhere to the City of Los Angeles Information Security Policy. In addition, City-issued devices must have malware protection that is regularly updated.

The Virtual & Augmented Reality topic above was prepared by Anthony Moore, Deputy Chief Information Officer over Infrastructure at the City of Los Angeles Information Technology Agency. Anthony has over 25 years of technical and managerial IT experience, working across multiple government agencies, telecommunications, and a healthcare company.

OUR COMMITMENT TO LOS ANGELES

As Information Technology professionals at the City of Los Angeles, we are committed to serving the residents and businesses of Los Angeles by building thoughtful, human-centric technology solutions that are easy to use, cost-effective, and secure, through competitive contracting. Each year, our Information Technology Policy Committee (ITPC) will review this Digital Code of Ethics to ensure they are up-to-date and align with our digital values.

In our commitment to Los Angeles, we will hire an IT workforce that is as diverse as Los Angeles itself, and use technology to build bridges between City government and underserved communities.

We are committed to upholding the values and standards explained in this Digital Code of Ethics to build public trust, while deploying innovative and ethical technology solutions.

City of Los Angeles Departments

Aging
Airports
Animal Services
Building & Safety
Cannabis Regulation
Chief Legislative Analyst
City Administrative Officer
City Attorney
City Clerk
Civil & Human Rights
Community Investment for Families
Controller’s Office
Convention & Tourism Development
Cultural Affairs
Disability
Economic & Workforce Development
El Pueblo de Los Angeles
Emergency Management
Employee Relations Board
City Ethics Commission
Office of Finance
Los Angeles City Fire Department
Fire and Police Pensions
General Services
Harbor
Housing Authority
Los Angeles Housing Department
Information Technology Agency
Library
LA City Employee Retirement System (LACERS)
Mayor’s Office
Neighborhood Empowerment
Office of Public Accountability
Personnel
City Planning
Los Angeles Police Department
Board of Public Works
Public Works, Bureau of Contract Administration
Public Works, Bureau of Engineering
Public Works, Bureau of Sanitation
Public Works, Bureau of Street Lighting
Public Works, Bureau of Street Services
Recreation & Parks
Transportation
Water and Power
Youth Development
Zoo

CONTACT US

For questions, comments, or concerns about digital ethics at the City of Los Angeles, please contact the Information Technology Agency through the LA City website (https://www.lacity.org/submit-feedback).

For potential fraud or abuse, please contact the anonymous Fraud, Waste, and Abuse Hotline from the Controller's Office (https://lacontroller.org/report-fraud-waste-and-abuse/).

For City of Los Angeles IT managers and staff who are looking to assess or discuss the ethics of a specific technology or initiative, please request the item be added to the agenda of the Information Technology Policy Committee (ITPC) so we can discuss it as a group. The ITPC is a safe space for IT professionals to discuss the ethics of existing or upcoming digital initiatives.

NOTE - This Digital Code of Ethics shall be read to be consistent with federal, state, and local law. In addition, the Digital Code of Ethics shall not be read to create any right or benefit that is enforceable by any party against the City of Los Angeles, its officers, employees, departments, or bureaus.

City of Los Angeles
Artificial Intelligence Safety Checklist
September 2024

Overview

Artificial Intelligence (A.I.) offers tremendous opportunities to positively transform both the quality and quantity of services to City of Los Angeles residents, businesses, and visitors. However, the power of A.I. tools also stresses the importance of A.I. safeguards, digital ethics, and human-centered policies to prevent unintended harm to City operations or L.A.'s diverse communities. As the government of the people of the City of Los Angeles, it is our responsibility to be informed, aware, effective, and guarded with any emerging technologies that hold such promise and risk.

The Purpose of the A.I. Safety Checklist

This checklist was developed by the citywide Information Technology Policy Committee (ITPC) as a tool for departments to ensure due diligence and thoughtful examination before, during, and after the implementation of A.I. tools. This checklist will help City of Los Angeles Departments ensure that all A.I. tools adopted by the City of Los Angeles are implemented in as ethical, transparent, human-centered, and secure a process as possible. For any questions, please contact the Information Technology Agency IT Policy Committee Coordinators at ITA.ITPCCoordinators@lacity.org and they will forward your question to the appropriate party.

A.I. Safety Checklist

Where specified below, A.I. tool refers to both the A.I. software and its underlying infrastructure:

A. LEGAL COMPLIANCE & ETHICAL REQUIREMENTS

a. *Compliance with Legal and Ethical Standards* (ensure A.I. tool adheres to local, state, and federal regulations):

i. ☐-This A.I. tool complies with the values and recommendations of the *City of Los Angeles Digital Code of Ethics*

ii. ☐-This A.I. tool complies with all relevant laws and regulations, including but not limited to those related to data protection, privacy, and anti-discrimination

b. *Bias Mitigation & Accessibility* (safeguards to detect and reduce biases in data, algorithms, and outcomes):

i. ☐-If specialized datasets were created for this A.I. tool, then an analysis will be performed to ensure that demographic biases (e.g., race, gender, socioeconomic status, etc.) are not reflected in the A.I.'s decisions prior to launch, and periodically thereafter to identify, report, and mitigate any biases that may emerge after implementation

ii. ☐-If specialized datasets were created for this A.I. tool, then a periodic audit of these models will be performed to identify, report, and mitigate any biases that may emerge after implementation

iii. ☐-If specialized datasets were created for this A.I. tool, then fairness checks were conducted for each significant demographic group to ensure consistent, equitable outcomes prior to launch, and periodically thereafter to identify, report, and mitigate any biases that may emerge after implementation

iv. ☐-This A.I. tool meets accessibility standards for its expected user base, including the most recent Web Content Accessibility Guidelines (WCAG), and is periodically reviewed to ensure continued compliance with evolving best practices

c. *Human Oversight* (mechanisms for human intervention in decision-making processes, where necessary):

i. ☐-Human-in-the-loop mechanisms are integrated into this A.I. tool where A.I. decisions have significant consequences, such as in public safety or allocation of City services

ii. ☐-The responsibilities of human supervisors to override or adjust A.I. decisions when necessary, especially in complex or high-risk situations, are clearly defined

B. TRANSPARENCY & EXPLAINABILITY REQUIREMENTS

a. *Algorithm Transparency* (identify how the tool's algorithms work, including key decision-making processes):

i. ☐-Custom-built Vendor Tool (as defined in L.A. A.I. Roadmap) algorithms and decision-making processes should be documented, ensuring stakeholders can understand logic behind decisions

   ii. ☐-This A.I. tool will include a high-level description for public awareness, ensuring city residents can understand how A.I. is used in this case

b. *Data Transparency* (info on data used to train the A.I.):

   i. ☐-This A.I. tool discloses the source of the data used to train the A.I., specifying whether it comes from public datasets, proprietary sources, or is collected via city services

   ii. ☐-This A.I. tool points to an easy-to-understand data privacy policy that informs users about how their data is collected, stored, and used by the A.I. (if at all)

c. *User Notifications* (if publicly accessible, inform users when they are interacting with an A.I. tool):

   i. ☐-A.I. tool will inform City residents, visitors, businesses, partner agencies, or other external stakeholders when they are interacting with an A.I. system

   ii. ☐-A.I. tool includes a method for submitting feedback or appealing decisions made by the A.I. system

C. HUMAN-CENTERED DESIGN REQUIREMENTS

a. *Impact on Human Decision-Making* (ensure A.I. tool enhances, not replaces, human decision-making):

i. ☐-This A.I. tool has been assessed for how it enhances human decision-making without undermining human judgment, particularly in sensitive topics. For A.I. tools with publicly accessible components or that are making decisions directly impacting the public, this should include some form of community engagement (e.g. focus group, survey, etc) to ensure public feedback is solicited

ii. ☐-This A.I. tool is designed to ensure that human operators retain the ability to override the A.I. in exceptional cases, and that A.I. is augmenting human expertise, not replacing it

iii. ☐-This A.I. tool is designed to augment human capabilities, rather than replace human jobs

iv. ☐-This A.I. tool includes documentation for use and training for the employees maintaining and deploying the system.

D. SECURITY & DATA PRIVACY REQUIREMENTS

a. *Data Security Measures* (ensure security and privacy to protect against breaches and unauthorized access):

i. ☐-This A.I. tool, and its underlying infrastructure, adheres to the City of Los Angeles Information Technology Security Policy, including applicable data encryption and anonymization requirements and cybersecurity safeguards based on the type of A.I. system and data accessed

ii. ☐-This A.I. tool includes regular updates and patches necessary to address potential vulnerabilities, especially if it handles sensitive data

iii. ☐-This A.I. tool implements security protections, applying strong technical mitigations, where possible, to enforce the other checklist items

iv. ☐-This A.I. tool adheres to principles of data minimization such that it only collects or uses personal data when absolutely necessary, only for the intended purposes, and only retains that data for so long as necessary to fulfill the purposes for which it was collected or as required by law. This applies throughout this A.I tool's architecture, from the amount of data it accesses, to data shared with its servers, to data that might be shared with third parties

b. *Robustness Against Cyber Attacks* (safeguards to protect the A.I. tool from cyber threats, including hacking):

i. ☐-When public facing, this A.I. tool is included in the *Cyber Watch List* for frequent vulnerability scans

E. PERFORMANCE REQUIREMENTS

a. *Performance Validation* (validate the A.I. tool's accuracy, reliability, and performance in real-world scenarios to ensure it meets its intended goals):

i. ☐-This A.I. tool was tested in both controlled environments and real-world applications, ensuring that it performs as expected across a range of scenarios

ii. ☐-This A.I. tool was validated for its A.I. predictions, decisions, or outputs in comparison to human experts (where possible), to help ensure accuracy and reliability

iii. ☐-This A.I. tool will be validated periodically for its A.I. predictions, decisions, or outputs in comparison to human experts (where possible)

City of Los Angeles

Artificial Intelligence Tool Request Form

This form is developed for City of Los Angeles departments seeking to implement a new Artificial Intelligence (A.I.) Tool to request a review by the Information Technology Agency (ITA).

Date:	Department:
Requester Name:	Title:
Phone:	Email:

A.I. Tool Name:

Description:

Purpose / Benefits:

Questionnaire:

1. Is the A.I. Tool an internal tool for City employees or is it a public facing tool for residents, visitors, businesses, etc.? ____
    a. If internal, does it involve other City departments? If so, which?
    ____
    b. If external, please describe the target audience:
    ____
2. Is the A.I. Tool an out-of-the-box tool, custom tool, or tool integrated into existing application?
    ____
3. Is this service/license already implemented/available by another department? (Y/N)
4. Is the A.I. Tool a component of another City application? (Y/N)
5. Please describe your implementation, maintenance, and support strategies:
    ____
6. Is a proof of concept developed to demo at the Information Technology Policy Committee? (Y/N)
7. Please confirm the proposed A.I. Tool complies with Citywide IT Policies and Guidelines (link), including but not limited to the Information Security Policy and the Web Policy & Standards. (Y/N)
8. Please confirm the proposed A.I. Tool complies with the A.I. Safety Checklist (**link**) developed by the ITPC to ensure A.I. tools adopted by the City of Los Angeles are implemented in as ethical, transparent, human-centered, and secure a process as possible. (Y/N)