PRIVACY AND DISCLOSURE POLICY

The purpose of this document is to define the City of San José's policy and the requirements of its Contractors with regard to the collection and use of personally identifiable information (PII) collected, processed, or otherwise used in the course doing business with the City. Non-PII (i.e., anonymous information) and PII are defined below, followed by the requirements for City contracts where PII is used in the course of doing business with the City.

1 ANONYMOUS INFORMATION

This type of information does not identify specific individuals and is automatically transmitted and consists of:

- The URL (Uniform Resource Locator or address) of the web page a user previously visited.
- Unique "session IDs" randomly assigned to a user when accessing City WiFi. These IDs do not connect to the IP address (i.e., digital PII) of the device used to access the Internet and are randomly generated each time an individual logs on to City WiFi.
- The browser version users are using to access the site.

This information is used to help improve the City's systems, and none of the information can be linked to an individual.

2 PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally identifiable information (PII) includes any information that can directly or indirectly identify an individual, such as one's name or address. Refer to the table below for types of PII. A more extensive list of PII can be found in the Appendix attached to the end of this policy.

Category of PII	**Sub-categories**
Personal Data	Full name; Home address; Email address; Phone number; Phone, laptop, or other device internet protocol (IP) address; Government-Issued ID # (e.g., Driver's License, Passport, Social Security Number, FEIN); Employer ID number; License Plate; Credit or debit card information; Bank account, brokerage account or other financial information; Date of birth; Place of birth; Other written or scanned information that can directly tie to an individual or household
Sensitive PII or demographic-related PII	Biometric data; Genetic data; Physical identifiable characteristics; Other health records; Race or ethnic origin; Nationality;

Category of PII	Sub-categories
	Immigration status; Religious affiliation; Political affiliation; Voter status; Education records; Criminal records; Online activity and tracking, including cookies, pixels, usernames and passwords, or other online activity; Other sensitive information traditionally kept confidential ***NOTE:** Data is not considered PII if only shared in aggregate of a population larger than 1,000[1] (e.g., # of registered voters in San José)
Image data	Picture that can identify an individual by their face or other physical and contextual information[2]
Recording data	Video that can identify an individual by their face or other physical and contextual information; Audio that can identify an individual by their voice or other contextual information
Geolocation data	Data affiliated with a vehicle, computer, or other device that can be used to identify an individual's physical location

The City may determine, in its sole discretion, that other information is sensitive or PII. If the City determines information that is collected, processed, or otherwise used in the course of doing business with the City is PII, Contractor shall treat new pieces of this information as PII no later than 60 days following written notification from the City unless an extension is approved in writing. Following this written notification, all future information of this type shall be considered PII.

3 PROTECTION AND ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION

The City and Contractor shall make every reasonable effort to protect City and individual privacy. The City and Contractor will only collect personally identifiable information that is required to provide services. Users can decline to provide any personal information. However, if a user declines to provide requested information, the City and Contractor may not be able to provide the user with services dependent upon the collection of that information.

The City does not intentionally disclose any personal information provided by the Contractor to any third parties or outside the City except as required by law or by the consent of the person providing the information.

Access to personally identifiable information in the City's public records is controlled primarily by the California Public Records Act (Government Code Section 6250, et. seq.). Information that is generally available under the Public Records Act may be posted for electronic access through the City's Web Site. While the Public Records Act sets the general requirements for

[1] Based on reporting requirements used for anonymity by the U.S. Department of Health and Human Services AFCARS Foster Care Dataset; refer to the 2021 codebook, element #6.

[2] An example of "contextual information" being used to identify someone could include a picture of a license plate or a picture of someone's back next to a house with a visible address.

access to City records, other sections of the California code, as well as federal laws, also deal with confidentiality issues. Additional access to PII may be granted under the direction of local, state, or federal courts or under the direction of the San José City Council in compliance with local, state, or federal laws.

4 SECURITY

The City of San José is committed to data security and the data quality of personally identifiable information that is either available from or collected by City systems and has taken reasonable precautions to protect such information from loss, misuse, or alteration. When handling sensitive personally identifiable information, Contractor shall follow security measures outlined in relevant law and the City's security standards, as well as the City's Information Technology and Security Requirements.

5 REQUIREMENTS FOR CONTRACTORS WHEN HANDLING DATA

"Data" shall be defined as all data and information generated, collected, developed, discovered, or otherwise saved exclusively for the City.

To the extent permissible by law, Contractor shall adhere to the following requirements for protecting individual privacy while collecting, storing, sharing, processing, or otherwise handling any information they may have access to in the course of doing business with the City:

5.1 Notice to End User (hereinafter "User")

Outside the domain of first responder emergency response efforts, Contractor shall provide "notice at collection" as defined by the California Consumer Privacy Act, listing all PII collected, used, and shared by the data subject. Contractor shall provide such notice in terms that a layperson can understand them. Contractor must provide notice in at least the following languages: Spanish, Vietnamese, English.

If the Contractor does not collect PII on behalf of the City, such as in the case of a database management system with no collection service, the Contractor is not required to provide any notice.

5.2 Minimization

Contractors shall only collect, process, and share the minimum amount of PII required to carry out the designated services on behalf of the City. If the City determines the Contractor is handling more PII than is required, the Contractor must reduce PII collection to the amount determined by the City. All PII that was previously collected that is not deemed necessary by the City for the designated services shall be purged. Failure to reduce and purge data within 30 days of request will be considered a breach of contract unless the City grants an extension.

5.3 Accountability

Contractors shall maintain and provide evidence of compliance with this Privacy and Disclosure Policy upon request by the City.

5.4 Accuracy

Unless otherwise prohibited by local, state or federal law, rule or regulation, a User and the legal guardians of a User of the Contractor's services will be granted by the Contractor the ability to access and correct personally identifiable information used or stored by the Contractor after the Contractor verifies the User is the subject of the relevant personally identifiable information.

If the Contractor is notified by the City or a User of a discrepancy in its information handled on behalf of the City, Contractor shall verify its existing information and, if found incorrect, correct or delete the inaccurate information within 30 days of notification or request an extension from the City in writing. If notified by a User, the Contractor will inform the User when their data has been verified, corrected, or deleted.

5.5 Equity

Contractor shall take reasonable steps to advance equity and mitigate the impact of algorithmic bias through its data and information services while ensuring that PII is only used in accordance with this Agreement. "Reasonable steps" are those set forth in the National Institute of Technology's "Proposal for Identifying and Managing Bias in Artificial Intelligence" and follow-on published technical guidance starting in 2022, referenced herein and incorporated by reference. The City may at any time audit all information, processes, and analyses or request the Contractor anaylze the potential areas of algorithmic bias within or related to the services the Contractor provides to the City.

5.6 Monitoring and Auditing of Contractor Security and Privacy Performance

The City retains the right to observe or audit any relevant work processes, services, or documents in the course of doing business with the City to confirm that the Contractor (and any relevant sub-contractors) is complying with this Privacy and Disclosure Policy. Contractor shall provide access to information, documentation, and personnel required to complete this audit at no additional cost to the City.

6 REQUIRED DISCLAIMER

City systems provided through a Contractor shall contain a User disclaimer (terms of use) substantially containing the following information:

6.1 Provision of Service

The City of San José ("City") is not liable for any delays, inaccuracies, errors, or omissions relating to material contained or posted on this website, system, or within the services provided (collectively the "City Systems"). City Systems and all materials contained on them are distributed and transmitted "as is" without warranties of any kind, either express or implied, including without limitations, warranties of title, or implied warranties of merchantability or fitness for a particular purpose. The City is not responsible for any special, indirect, incidental, or consequential damages that may arise from the use of, or the inability to use, the City Systems and/or the materials contained on the City Systems whether the materials contained on the City Systems are provided by the City or a third party. The City is neither responsible nor liable for any viruses or other contamination of user's system.

6.2 Access to Information

Unless otherwise prohibited by state or federal law, rule or regulation, user will be granted the ability to access and correct any personally identifiable information. The City and/or its Contractors will verify user's identity before granting such access. Each service provided that collects personally identifiable information will allow for review and, upon verification, update of that information.

6.3 Non-City Systems

Non-City Systems may be linked through City Systems. The City is not responsible for any non-City Systems, which may or may not be subject to the Public Records Act and may or may not be subject to the San José Municipal Code, California law, or federal law. Visitors to such websites are advised to check the privacy statements of such sites and to be cautious about providing personally identifiable information without a clear understanding of how the information will be used.

6.4 City Liability

The City is not responsible for, and accepts no liability for, the availability of non-City Systems and/or resources. Linked systems are not under the control of, nor maintained by, the City, and the City is not responsible for the content of these systems, which may change frequently. In addition, inclusion of the linked systems does not constitute an endorsement or promotion by the City of any persons or organizations affiliated with the linked systems.

APPENDIX: PII REFERENCE LIST

This PII Reference List includes 6 categories and types of PII and subsets of PII that are included when the City refers to "personal" or "sensitive" data or information.

Personally Identifiable Information (PII)
First Name
Last Name
Alias Name
Maiden Name
Full Home Street Address
Zip Code
Date of Birth
Date of Death
Email Address
Photograph
Internet Protocol (IP) Address
Marital Status
Beneficiary Name
Beneficiary Contact Phone Number
Beneficiary Contact Address
Employee ID
Identifying Marks (e.g. tattoos, birth marks, etc.)
Identifying information of children, youth, minors under 18 year old
SSN (full 9 digits)
Driver's License Number
Vehicle Information (license plate #, vehicle ID# (VIN))
Passport Number
State or City ID Number
Criminal Justice Number (arrestee or prisoner numbers)
Username/ID
User Hint Question and Answer
Biometric ID Data (fingerprint, iris scan, faceprint, etc.)
Voter ID Number
FEIN (Federal Employer Identification Number)
Alien Registration Number

Demographics Subset
Citizenship Status
Nationality
Sexual Orientation
Gender Identity

Background Check/Investigation Details or Results
Drug and Alcohol Abuse Information
Criminal Offenses/Convictions
Physical Characteristics
Political Party Affiliation
Political Party Affiliation
Military / Veteran Status
Race / Ethnic Origin
Religious / Philosophical Beliefs

Other Sensor Information
Audio Recordings
Phone Call Recordings
Video Recordings
Social Network Profile, Family Network Research and/or Friends/Contacts/Followers
Computer Use or Website Tracking/ Monitoring (cookies, web beacons, web widgets)
Location Tracking (individual or vehicle, geo-location, RFID Tracking, cell tower data)
Behavioral Pattern Mapping (e.g. physical, psychological, online, etc.)
Item or Identifier Scanning (contraband recognition, license plate reader, RFID reader)
Other Electronic Signatures or Monitoring (other cell phone signal, device sensors monitoring usage not previously stated)
Other Sensory Data (visual, audio, olfactory, or biometric not previously stated)
Other uncategorized surveillance information or data

Health Information Subset
Relative / Emergency Contact Name
Relative / Emergency Contact Phone Number
Relative / Emergency Contact Email
Relative / Emergency Contact Address
Disability Description
Health Diagnosis or Condition for Physical / Mental Health (non-substance use)
Health Diagnosis (substance use)
Health Services Provided
Medical Record Number
Health Plan / Insurance ID Number or Policy (inc. Medicaid & Medicare)
Medical Payments or Health Insurance Payments (incl. Medicaid & Medicare)
Health Policy Group Number
Patient ID Number
Medical Records
Prescriptions / Medications

Financial Information Subset
Bank or Financial Account Number

Credit Card / Debit Card Number
Other Credit / Debit Card Data (eg. Expiration date, security code)
Personal Identification Number (PIN)
Personal Check Data or Scanned Images
Income/Salary/Wage Data
Socio-Economic Status
Credit Score, Credit Grade, or Credit History

Other Sensitive Information (organizational, children, unstructured)
Intellectual Property or Proprietary Information
Budgets, Financial Statements / Forecasts
Organizational Strategy, Business Decision, or Design Info
Legal Documents, Contracts, Vendor Agreements
Other Children's Information not previously stated
Other Confidential Information not previously covered
Any Unstructured Data that might include any of the above types of information