Shared Micro-Mobility Permit Data Protection Principles

Per the City's Shared Micro-Mobility Permit, San José DOT (DOT) requires micro-mobility Operators ("Operators") to comply with the Micro Mobility Data Specification (MDS) to set a consistent standard for the transfer, use, and protection of vehicle data from Operators to the City of San José through its selected mobility data processing vendor ("Vendor").

DOT will apply the following data protection principles ("Principles") to all data obtained from permitted Operators ("City Data") or through third party vendors to ensure the protection of personal privacy and personally identifiable data as well as protection and security of City Data. These Principles are in accordance with the City's Digital Privacy Principles,[1] and the applicable standard privacy and disclosure policy governing mobility data vendor contracts for the management of MDS vehicle data.[2]

1. Data Protection

DOT will take appropriate administrative, physical, and technical safeguards to properly secure and assure the integrity of data provided by Operators, including contracting a vendor to safely consume, analyze, store, and manage MDS data. In addition to these Principles, Appendix B details the terms and conditions for the use of City Data by Vendors as well as the terms of use of data processing software by the City.

2. Data Minimization

DOT will analyze data only for enforcement and planning purposes in furtherance of its responsibilities to oversee the shared micro-mobility permit program and ensure public safety. DOT will not access personally identifiable information and will require that Vendors implement methodologies for aggregation comparable to Shared Streets,[3] and/or in accordance with the most current industry best practices for vehicle data aggregation.

3. Access and Purpose Limitation

DOT will limit access to trip data provided by Operators to what is required for the City's operational and regulatory needs as established by the Shared Micro-Mobility Permit Administrative Regulations.[4]

3.1. City Data shall remain in the control of the City. Vendors do not acquire any rights to City data, other than to provide services to the City.

3.1. City Data shall not be used for secondary purposes, other than to provide services to the City.

3.3. City Data shall not be copied, disclosed, or retained by Vendors for use in any process, publication, or transaction other than to provide services to the City.

[1] San Jose Digital Privacy Principles, https://www.sanjoseca.gov/your-government/city-manager/civic-innovation-digital-strategy/digital-privacy
[2] See Appendix A, Shared Micro-Mobility Data Analytics Platform RFQ Privacy and Disclosure Policy
[3] Shared Streets Mobility Metrics, https://sharedstreets.io/mobility-metrics/
[4] SMM Permit Administrative Regulations, https://www.sanjoseca.gov/home/showdocument?id=38091

3.4. Vendors shall use all reasonable efforts to prevent unauthorized uses of City Data at any time, safeguard Data confidentiality and integrity, and shall meet the following conditions:

3.4.1. Vendors handling City Data shall implement and maintain appropriate administrative, technical, and organizational security measures in order to safeguard against unauthorized access, disclosure, or theft of Data.

3.4.2. Unless otherwise stipulated, vendors shall encrypt all Data at rest and in transit with controlled access.

3.4.3. Vendors shall apply and support encryption solutions that are certified against U.S. Federal Information and Processing Standard 140-2, Level 2, or equivalent industry standard, and verify that the encryption keys and keying material are not stored with any associated Data.

3.4.4. Storage of City Data shall be located in the continental United States of America.

3.4.5. Vendors shall use precautions, including, but not limited to, physical software and network security measures, personnel screening, training and supervision, and appropriate agreements to: (1) prevent anyone other than the City and Vendors' personnel with a specific need to know, from gaining access to City Data; (2) protect Data from loss, corruption, or unauthorized alteration; and (3) prevent the disclosure of City and Vendor's usernames, passwords, API keys, and other access control information to anyone other than authorized City personnel.

3.5. Vendors shall implement the following security controls with respect to City Data and to any service provided to the City: (1) authorize access only to the minimum number of personnel required for a function; (2) divide functions among its personnel to reduce the risk of one person committing fraud undetected; (3) restrict access to vendors' authorized users and base access control on the role users play in the vendor organization.

3.6. Vendors shall restrict the use of, and access to, administrative credentials for accounts and system services accessing City Data, to only those Vendor's personnel whose access is essential for the purpose of providing the contracted services to the City.

4. Security and Administration

DOT will require Vendors meet minimum security and administration safeguards for the management of City Data. Vendors shall:

4.1. Implement operational procedures and controls designed to ensure that technology and information systems are configured and maintained according to prescribed internal standards and consistent with applicable industry standard safeguards such as ISO/IEC 27002:2005, NIST 800-53, 800-44, Microsoft Security Hardening Guidelines, OWASP Guide to Building Secure Web Applications, SOC 2 Type 2, and the various Center for Internet Security Standards.

4.2. Employ vulnerability management and regular application, operating system, and other infrastructure patching procedures and technologies designed to identify, assess, mitigate, and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code.

4.3. Have, implement, and maintain network security controls, including the use of firewalls, layered DMZs and updated intrusion, intrusion detection and prevention systems, reasonably designed to protect

systems from intrusion or limit the scope or success of any attack or attempt at unauthorized access to City Data.

4.4. Continuously monitor their networks and personnel for malicious activity and other activity that may cause damage or vulnerability to City Data.

4.5. Establish and maintain a formal, documented, mandated, company-wide Data Security Policy.

4.6. At least annually, perform vulnerability tests and assessments of all systems that contain City Data.

5. Backups and Storage

5.1. Vendors shall employ a multilayered approach to backups and disaster recovery including the use of a primary data center and a backup data center. Vendors shall perform both local and remote backups of the complete server infrastructure including server operating systems, applications, and data.

5.2. At the conclusion of an agreement with the City, Vendors shall return, delete, or destroy data in their possession or under their control.

5.3. Vendors shall implement and utilize appropriate methods to ensure the destruction of City Data. Such methods shall be in accordance with recognized industry best practices and shall leave no City Data recoverable on Vendors' computers or other media.

5.4. In case of a data breach, Vendors shall notify the City as soon as reasonably feasible, but in any event within forty-eight hours after discovery of any breach.

Appendix A

Shared Micro Mobility RFQ 1907-001 Privacy and Disclosure Policy

The purpose of this statement is to define the City of San José's policy with regard to the collection and use of personally identifiable information (PII). PII is any information relating to an identified or identifiable individual who is the subject of the information. Users of the City Web Site should be informed of the following:

The City of San José collects two kinds of customer information: (1) anonymous and (2) personally identifiable information (PII).

1. Anonymous information

This type of information does not identify specific individuals and is automatically transmitted by City browser. This information consists of:

- The URL (Uniform Resource Locator or address) of the web page user previously visited.
- The domain names and/or IP addresses which are numbers that are automatically assigned to City computer whenever user is connected to the Internet or World Wide Web.
- The browser version user is using to access the site. This information is used to help improve the City's Web Site. None of the information can be linked to an individual.

2. Personally Identifiable Information (PII)

This type of information could include name, address, email address, telephone number, and credit/debit card information. The City will make every reasonable effort to protect costumer privacy. It restricts access to customer personal identifiable information to those employees who will respond to City request. The City does not intentionally disclose any personal information about Contractor customers to any third parties or outside the City except as required by law or by the consent of the person providing the information.

The City only collects personally identifiable information that is required to provide service. A City Website user can decline to provide us with any personal information. However, if user elects to withhold requested information, the City may not be able to provide user with the certain online services dependent upon the collection of that information.

3. Access to Personally Identifiable Information

Access to personally identifiable information in public records at local levels of government in San José 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 policies for access to City records, other sections of the California code as well as federal laws also deal with confidentiality issues.

4. Email addresses

Email addresses obtained through the City's Web Site will not be sold or given to other private companies for marketing purposes. The information collected is subject to the access and confidentiality provisions of the Public Records Act, other applicable sections of the California code as well as Federal laws. Email

or other information requests sent to the City Web Site may be maintained in order to respond to the request, forward that request to the appropriate Department within the City, communicate updates through the City's page that may be of interest to citizens, or to provide the City web designer with valuable customer feedback to assist in improving the site. Individuals can cancel any communications regarding new service updates at any time.

5. Use of "Cookies"

Some City applications use "cookies." A cookie is a small data file that certain web sites write to the City's hard drive when a user visits them. A cookie file can contain information such as a user id that the site uses to track the pages a user has visited. But the only personal information a cookie can contain is information supplied by the user. A cookie is only a test file and cannot read data off a user's hard disk or read cookie files created by other sites. Cookies can track users' traffic patterns, recognize users' computer browser when a user returns, and could provide personalized content without requiring sign-in.

Users can refuse cookies by turning them off in their user browser. However, Cookies may be required to use some of the web applications on the City's Web Site.

6. 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 the City's Web Site, and has taken reasonable precautions to protect such information from loss, misuse, or alteration.

7. Contractual Services for the City's Web Site and On-Line Services

To insure that contractors who have access to or provide contractual services for the City's On-Line (e-government) Services are not allowed to re-sell, or in any way share or convey to another party, or use it for another purpose, any information that they may have access to in the course of doing business for the City; all city contracts regarding such services should contain a requirement that the contractor must comply with the City's Web Site and e-Government policies.

8. Electronic Signatures and Payments

The City of San José is committed to data security and data quality of personally identifiable information that is either available from or collected by Contractor web site, and has taken reasonable precautions to protect such information from loss, misuse, or alteration. When a City application accepts credit cards or any other particularly sensitive information for any of its services, it encrypts all ordering information, such as the customer's name and credit card number, in order to protect its confidentiality.

9. Disclaimer

The City Web Site should contain a disclaimer substantially containing the following information:

9.1. The City of San José is neither responsible nor liable for any delays, inaccuracies, errors, or omissions arising out of users' use of the City's Web Site, or with respect to the material contained on the Site, including, without limitation, any material posted on the Site; nor for any viruses or other contamination of users' systems. The City Web Site and all materials contained on it are distributed and transmitted "as is" without warranties of any kind, either expressed or implied, including, without limitations, warranties of title or implied warranties of merchantability or fitness for a particular purpose. The City of San José is not responsible for any special, indirect, incidental or consequential damage that

may arise from the use of, or the inability to use, the Web Site and/or the materials contained on the Web Site, whether the materials contained on the Web Site are provided by the City of San José or a third party. The City of San José is neither responsible nor liable for any viruses or other contamination of a user's system.

9.2. Access to Information. Unless otherwise prohibited by state or federal law, rule or regulation, users will be granted the ability to access and correct any personally identifiable information. The City will take reasonable steps to verify a user's identity before granting such access. Each City service that collects personally identifiable information will allow users to review, or review and update that information.

9.3. Non-City Web Sites. Non-city web sites may be linked through the City's Web Site. Many non-city sites may or may not be subject to the Public Records Act and may or may not be subject to other sections of the California code or federal law. Visitors to such sites 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.

9.4. The City is not responsible for, and accepts no liability for, the availability of these outside resources. Linked Web sites are not under the control of, nor maintained by, the City and the City is not responsible for the content of these Web sites, which can and do change frequently; nor for any internal links the displayed Web sites may contain. In addition, inclusion of the linked Web sites does not constitute an endorsement or promotion by the City of any persons or organizations sponsoring the displayed Web sites.

Appendix B

Terms and Conditions of City Data License and Use of Data Software

1. Ownership and Intellectual Property

1.1. City Data. Vendors have no ownership of and, except as stated in the Principles and this Appendix, acquire no rights in City Data. As between the City and Vendors, City retains all right of ownership, title, and interest in and to City Data, including all intellectual property rights therein.

1.2. Data analytics. Vendors may use their own data, such as usage and statistics data, as well as de-identified and aggregated data so that such data does not identify any person or any Operator to provide, maintain, and improve their services to the City and develop new features and services for the City.

1.3. Intellectual Property. The City retains all rights of ownership, title, and interest in and to any reports and other work products prepared by the City when processing City Data through Vendors' software, except that Vendors retain ownership and reserve all rights, title and interest in and to their software and any modification and improvements thereof.

2. City Data License

2.1. City Data License to Vendors. Subject to the terms contained in the Principles, the City grants Vendor a non-exclusive and revocable license to use, analyze, create derivative works based on, host, store, display and process City Data, solely for the purpose of performing, maintaining and improving the services to the City for the duration of the Vendor's term of engagement. Additionally, Vendors may use de-identified City Data (aggregated data such that no individual Operator can be identified or associated with the data) including performance metrics, statistics, and usage data solely to improve their services or offer new services to the City. Vendors shall not use, analyze, host, store, or process City Data for any other purpose.

2.2. Sandbox data. Vendors will also receive data from Operators in a sandbox testing environment to test any modifications in the data feed from the Operators.

2.3. Operators' access. In furtherance of transparency, at Operators' request and pursuant to a separate agreement with each interested Operator, Vendors may give access to the datasets of that particular Operator only, representing information the City has available on that Operator through Vendor's data processing software.

2.4. Suggestions. Vendors may use, modify and incorporate City suggestions and feedback regarding Vendors' software into Vendors' products and services.

3. Use of Data Processing Software by The City

3.1. Software License. Subject to the terms of this Appendix, Vendor grants to the City, and the City accepts, for the duration of the term of the Vendor's engagement, a non-exclusive, non-transferable license for the territory of Greater San Jose, to use Vendor's software to visualize, process, analyze, store, and export City Data.

3.2. Access to the Software. The Vendor will assign to City Users selected by the City unique necessary usernames and passwords, which will control and allow access to the Software and which shall be kept confidential by the City and said City Users. Each username and password will be for the personal use of

a single selected City User only. The Vendor will promptly change the passwords upon City's request. The City shall promptly notify the Vendor to deactivate the access to the software for those City Users whose employment with the City will terminate or who otherwise no longer should have access to the software. The term "City Users" means city employees, interns, and any other persons by prior written agreement between the City and the Vendor. City consultants and other third parties' access to the software shall be governed by a separate software license between the Vendor and such consultants and third parties.

3.3. Inconsistencies in the MDS implementation. For sending data generated by using the software by the City, to the extent there are any inconsistences between the Vendor's software and any other software in implementation of policies, geographies, reports, audit, metrics, etc., Vendor's implementation prevails.

3.4. Responsibilities of the City. The City is responsible for the use of the software by the City and City Users. The City will make reasonable efforts to comply with its Data Protection Principles and to keep the City usernames, passwords, API keys and other credentials required to access the software secure and free from unauthorized access. The City shall promptly notify a Vendor of any unauthorized use of the software.

3.5. Restrictions. The City will not allow any City User to: (a) reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code or underlying ideas or algorithms of the Vendor's software, (b) modify or create derivative works based on the software, (c) sell, resell, license, copy, rent, lease, distribute, time-share the software or otherwise use the software for the benefit of a third party, (d) remove or alter proprietary notices from the software, or (e) use the software to create any product other than City reports and documents.

3.6. Exceptions to Section 3.5. The terms indicated in Section 3.5 do not apply to or prohibit the City from disclosing or discussing its experience with the software with other cities, governmental bodies, and governmental agencies. In addition, the restrictions indicated in Section 3.5 do not apply to any City reports or documents.

4. Confidentiality and Privacy

4.1. Definition of Confidential Information. "Confidential Information" shall be defined in the same way as in the applicable state or local laws or regulations followed by the City.

4.2. Obligations. Each Party shall use reasonable care to not use the other Party's Confidential Information for any purpose outside of the scope of the Vendor's engagement. Vendors may disclose the City's relationship with a Vendor to third parties.

4.3. Disclosure. Each Party may disclose the other Party's Confidential Information to enforce its rights or when required by law, including the California Public Records Act (CPRA) or other regulations, so long as the disclosing Party will use its best efforts to give a courtesy notice of the disclosure to the other Party prior to the disclosure.

4.4. Personal Information. It is the Parties' understanding that no personal information within the meaning of the California Consumer Privacy Act (CCPA) is part of the City Data. Nevertheless, both Parties are responsible for ensuring that performance of their obligations and exercise of their rights complies with the CCPA, to the extent it is applicable, and other applicable local, state, and federal privacy laws and regulations, as amended from time to time. To the extent the Parties are in possession, custody or control of any personal information outside City Data, including but not limited to any employee names, logins

and passwords to access the software, the Parties shall treat this personal information as Confidential Information and safeguard it and protect it from any unauthorized access, copying or disclosure.