DART Software as a Service Additional Terms and Conditions ("SaaS Terms")

Definitions

Agreement means the written agreement between Des Moines Area Regional Transit Authority ("DART") and contractor and into which these SaaS Terms are incorporated by reference.

Data means all information, whether in oral, written, or electronic form, created by or in any way originating with DART, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or that in any way originated with DART, in the course of using and configuring the Services.

Data Breach means any actual or reasonably suspected unauthorized access to or acquisition of Encrypted Data.

Encrypted Data means Data that is required to be encrypted under the Agreement.

IT Governance Documents means the State of Iowa's written policy and standards documents available at: https://ocio.iowa.gov/standards.

Security Incident means any actual or reasonably suspected unauthorized access to the contractor's system, regardless of whether contractor is aware of a Data Breach. A Security Incident may or may not become a Data Breach.

Service(s) means that which is provided to DART by contractor pursuant to the Agreement and the contractor's obligations under the Agreement.

Service Level Agreement means a written agreement between both DART and the contractor that is subject to the terms and conditions of the Agreement. Service Level Agreements should include: (1) the technical service level performance promises (i.e. metrics for performance and intervals for measure);
(2) description of service quality; (3) identification of roles and responsibilities; (4) remedies, such as credits; and (5) an explanation of how remedies or credits are calculated and issued.

Statement of Work means the written agreement between both DART and contractor attached to and incorporated into the Agreement.

Terms

1. **Data Ownership:** DART owns all rights, title, and interest in the Data. The contractor shall not access DART user accounts or Data, except: (1) in the normal course of data center operations; (2) in response to Service or technical issues; (3) as required by the express terms of the Agreement, applicable Statement of Work, or applicable Service Level Agreement; or (4) at DART's written request.

Contractor shall not collect, access, or use Data except as strictly necessary to provide Service to DART. No information regarding DART's use of the Service may be disclosed, provided, rented, or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of the Agreement.

2. **Data Protection:** Protection of personal privacy and Data shall be an integral part of the business activities of the contractor to ensure there is no inappropriate or unauthorized use of Data at any time. To this end, the contractor shall safeguard the confidentiality, integrity, and availability of Data and shall comply with the following conditions:

2.1. The contractor shall implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, or theft of Data. Contractor shall implement and maintain heightened security measures with respect to Encrypted Data. Such security measures shall be in accordance with OCIO practice and recognized industry practice, including but not limited to the IT Governance Documents.

2.2. All Encrypted Data shall be subject to controlled access. Any stipulation of responsibilities shall be included in a Statement of Work and will identify specific roles and responsibilities.

2.3. The contractor shall encrypt all Data at rest and in transit. DART may, in a Statement of Work, identify Data it deems as that which may be publicly disclosed that is not subject to encryption. Data so designated may be maintained without encryption at rest and in transit. The level of protection and encryption for all Encrypted Data shall meet or exceed that required in the IT Governance Documents.

2.4. At no time shall any Data or processes — that either belong to or are intended for the use of DART— be copied, disclosed, or retained by the contractor or any party related to the contractor for subsequent use in any transaction that does not include DART.

2.5. The contractor shall not use any information collected in connection with the Services for any purpose other than fulfilling its obligations under the Agreement.

3. **Data Location:** Storage of Data at rest shall be located solely in data centers in the United States and the contractor shall provide its Services to DART and its end users solely from locations in the United States. The contractor shall not store Data on portable devices, including personal laptop and desktop computers. The contractor shall access Data remotely only as required to provide technical support. The contractor shall provide technical user support on a 24/7 basis unless specified otherwise in the Service Level Agreement.

4. **Notice Regarding Security Incident or Data Breach:**

4.1. Incident Response: Contractor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries, and seeking external expertise as mutually agreed upon, defined by law, or contained in the Agreement. Discussing Security Incidents and Data Breaches with DART must be handled on an urgent basis, as part of contractor's communication and mitigation processes as may be more fully defined in the Service Level Agreement or the Agreement.

4.2. Security Incident Reporting Requirements: The contractor shall report a Security Incident to the DART-identified contact(s) as soon as possible by telephone and email, but in no case later than 48 hours after the Security Incident occurs.

4.3. Data Breach Reporting Requirements: If a Data Breach occurs, the contractor shall do the following: (1) as soon as possible notify the DART-identified contact(s) by telephone and email, but in no case later than 48 hours after the Data Breach occurs unless a shorter notice period is required by applicable law; and (2) take commercially-reasonable measures to address the Data Breach in a timely manner. Notice requirements may be clarified in the Service Level Agreement. If the Data involved in the Data Breach involves protected health information, personally identifying information, Social Security numbers, or otherwise confidential information, other sections of the Agreement may apply. The requirements discussed in those sections must be met in addition to the requirements of this section.

5. Responsibilities Regarding Data Breach:

5.1. The contractor shall: (1) cooperate with DART as reasonably requested

by DART to investigate and resolve the Data Breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document and provide to DART responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the Services, if necessary.

5.2. Unless stipulated otherwise in the Agreement or a Statement of Work, if a Data Breach is a result of the contractor's breach of its contractual obligation to encrypt Data or otherwise prevent its release as reasonably determined by DART, the contractor shall bear the costs associated with: (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators, or others required by federal and/or state law, or as otherwise agreed to in the Agreement or a Statement of Work; (3) a credit monitoring service required by federal and/or state law, or as otherwise agreed to in the Agreement or a Statement of Work; (4) a website or a toll-free number and call center for affected individuals required by federal and/or state law — all of which shall not amount to less than the average per-record per-person cost calculated for data breaches in the United States (in, for example, the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach); and (5) complete all corrective actions as reasonably determined by contractor based on root cause and on advice received from OCIO. If the Data involved in the Data Breach involves protected health information, personally identifying information, Social Security numbers, or otherwise confidential information, other sections of this contract may apply. The requirements discussed in those sections must be met in addition to the requirements of this Section.

6. **Notification of Legal Requests**: If the contractor is requested or required by deposition or written questions, interrogatories, requests for production of documents, subpoena, investigative demand or similar process to disclose any Data, the contractor will provide prompt written notice to DART and will cooperate with DART's efforts to obtain an appropriate protective order or other reasonable assurance that such Data will be accorded confidential treatment that DART may deem necessary.

7. **Termination and Suspension of Service**:

7.1. In the event of a termination of the contract, the contractor shall implement an orderly return of Data in a mutually agreeable and readable format. The contractor shall provide to DART any information that may be required to determine relationships between data rows or columns. It shall do so at a time agreed to by the parties or shall allow DART to extract its Data.

Upon confirmation from DART, the contractor shall securely dispose of the Data.

7.2. During any period of Service suspension, the contractor shall not take any action that results in the erasure of Data or otherwise dispose of any of the Data.

7.3. In the event of termination of any Services or contract in its entirety, the contractor shall not take any action that results in the erasure of Data until such time as DART provides notice to contractor of confirmation of successful transmission of all Data to DART or to DART's chosen vendor.

During this period, the contractor shall make reasonable efforts to facilitate the successful transmission of Data. The contractor shall be reimbursed for all phase-out costs (i.e., costs incurred within the agreed period after contract expiration or termination that result from the transfer of Data or other information to DART). The reimbursement rate shall be consistent with the then applicable rates set forth in the Agreement or a Statement of Work. After such period, the contractor shall have no obligation to maintain or provide any Data and shall thereafter, unless legally prohibited, delete all Data in its systems or otherwise in its possession or under its control. DART shall be entitled to any post-termination assistance generally made available with respect to the Services, unless a unique data retrieval arrangement has been established as part of a Service Level Agreement.

7.4. Upon termination of the Services or the contract in its entirety, contractor shall, within 30 days of receipt of DART's notice given in 7.3 above, securely dispose of all Data in all of its forms, including but not limited to, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to DART upon completion.

8. **Background Checks:** The contractor shall conduct a Federal Bureau of Investigation Identity History Summary Check for each employee involved in provision of Services: (1) upon commencement of the contract; (2) prior to hiring a new employee; and (3) for any employee upon the request of DART. The contractor shall not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to one (1) year is an

authorized penalty. The contractor shall promote and maintain an awareness of the importance of securing DART's information among the contractor's employees, subcontractors, and agents. If any individual providing Services under the contract is not acceptable to DART, in its sole opinion, as a result of the background or criminal history investigation, DART, in its sole option, shall have the right to either: (1) request immediate replacement of the individual; or (2) immediately terminate the contract, related Statement of Work, and related Service Level Agreement.

9. **Access to Security Logs and Reports:** The contractor shall provide to DART reports upon request, or on the schedule and in the format specified in the Agreement or the Service Level Agreement as agreed to by both the contractor and DART. Reports shall include latency statistics, user access, user access IP address, user access history, and security logs for all Data.

10. **Contract Audit:** The contractor shall allow DART to audit conformance to the contract terms. DART may perform this audit or contract with a third party at its discretion and at the DART's expense.

11. **Data Center Audit**: The contractor shall perform an annual independent audit of its data center(s) where Data, DART applications, or other DART information is maintained. The contractor shall perform this independent audit at its expense and shall, upon completion, provide an unredacted version of the complete audit report to DART. (The contractor may redact its proprietary information from the unredacted version, however.) A Service Organization Control (SOC) 2 audit report or equivalent approved by OCIO sets the minimum level of a third-party audit.

DART may perform an annual audit of contractor's data center(s) where Data, DART applications, or other DART information is maintained. The audit may take place onsite or remotely, at DART's discretion. DART shall provide to contractor thirty (30) days' advance notice prior to the audit. The contractor will make reasonable efforts to facilitate the audit and will make available to DART members of its staff during the audit. DART may contract with a third party to conduct the audit at its discretion and at DART's expense. If the contractor maintains Data, DART applications, or other DART information at multiple data centers, DART may perform an annual audit of each data center.

12. **Change Control and Advance Notice:** The contractor shall give notice to DART for change management requests. Contractor shall provide notice to DART regarding change management requests that do not constitute an emergency change management request at least two (2) weeks in advance of implementation. Contractor shall provide notice to DART regarding emergency change management requests no more than twenty-four (24) hours after

implementation.

Contractor shall make updates and upgrades available to DART at no additional cost when contractor makes such updates and upgrades generally available to its users. No update, upgrade, or other change to the Service may decrease the Service's functionality, adversely affect DART's use of or access to the Service, or increase the cost of the Service to DART.

13. **Security:** The contractor shall, on an annual basis, disclose its non-proprietary system security plans or security processes and technical limitations to DART such that adequate protection and flexibility can be attained between DART and the contractor. For example: virus checking and port sniffing. DART and the contractor shall share information sufficient to understand each other's roles and responsibilities. The contractor shall take into consideration feedback from OCIO with respect to the contractor's system security plans.

14. **Non-disclosure and Separation of Duties:** The contractor shall enforce role-based access control and separation of job duties, require commercially-reasonable nondisclosure agreements, and limit staff knowledge of Data to that which is absolutely necessary to perform job duties. The contractor, at DART's request, shall provide to DART a list of individuals who have access to the Data and/or the ability to service the systems that maintain the Data.

15. **Import and Export of Data:** DART shall have the ability to import or export Data in piecemeal or in entirety at its discretion, with reasonable assistance provided by the contractor, at any time during the term of the Agreement. This includes the ability for DART to import or export Data to/from other parties at DART's sole discretion. Contractor shall specify in a Statement of Work if DART is required to provide its own tools for this purpose, including the optional purchase of contractor's tools if contractor's applications are not able to provide this functionality directly.

16. **Responsibilities and Uptime Guarantee**: The contractor shall be responsible for the acquisition and operation of all hardware, software, and network support related to the Services being provided. The technical and professional activities required for establishing, managing, and maintaining the environments are the responsibilities of the contractor. Subject to the Service Level Agreement, the Services shall be available to DART at all times. The contractor shall allow DART to access and use the Service to perform synthetic transaction performance testing.

The contractor shall investigate and provide to DART a detailed incident report regarding any unplanned Service interruptions or outages. DART may terminate the Agreement or a Statement of Work for cause if, at its sole discretion, it determines that

the frequency of contractor-preventable outages is sufficient to warrant termination.

17. **Subcontractor Disclosure**: Contractor shall identify all of its strategic business partners related to Services, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the contractor, and who may be involved in any application development and/or operations.

The contractor shall be responsible for the acts and omissions of its subcontractors, strategic business partners, or other entities or individuals who provide or are involved in the provision of Services.

18. **Business Continuity and Disaster Recovery:** DART's recovery time objective shall be defined in the Service Level Agreement. The contractor shall ensure that DART's recovery time objective has been met and tested as detailed in the Service Level Agreement. DART may request the contractor shall provide to DART a business continuity and disaster recovery plan which details how DART's recovery time objective has been met and tested. DART may request the contractor work with DART to perform a disaster recovery test and take action to correct any issues detected during the test in a time frame mutually agreed upon between the contractor and DART.

DART's Data shall be maintained in accordance with the applicable DART records retention requirement, as determined by DART. The contractor shall annually provide to DART a resource utilization assessment detailing the Data maintained by the contractor. This report shall include the volume of Data, the file formats, and other content classifications as determined by DART.

19. **Compliance with Accessibility Standards**: The contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the State.