DART Data Privacy and Security Standards
Terms and Conditions

Data Privacy and Security

Entering into an agreement to become a Provider (hereinafter referred to as "Provider") for the Des Moines Area Regional Transit Authority (DART) involves the sharing of a significant amount of legally protected Personal Information such as Personally Identifiable Information (PII), Personal Health Information (PHI) and/or Personal Credit Information (PCI). The sharing of this information is necessary to enable the Provider to provide the services relevant to this Contract. The privacy of Personal Information is governed by a number of laws including the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information for Economic and Clinical Health Act (HITECH), the Fair Credit Reporting Act (FCRA), and the Children's Online Privacy Protection Act (COPPA); as well as other federal and state laws, regulations, common law privacy principles, and industry standards and guidelines. DART could face serious financial and/or reputational harm should there be an unauthorized use, a security incident, or a security breach. Therefore, the Provider shall conform to the following standards of care and obligations with respect to the treatment of Personal Information.

Definitions

"Authorized Employees" means the Provider's employees who need to know or otherwise access Personal Information to enable the Provider to perform their obligations under this Contract.

"Authorized Persons" means (i) Provider's Authorized employees; and (ii) Provider's independent contractors, vendors, agents, outsourcers, and auditors who need to know or otherwise access Personal Information to enable the Provider to perform their obligations under this Contract, and who are bound in writing by confidentiality obligations sufficient to protect Personal Information in accordance with the terms and conditions of this Contract.

"Highly Sensitive Personal Information" means (i) an individual's government-issued identification number (including Social Security number, driver's license number, or other state-issued identification number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number, or password that would permit access to an individual's financial account; (iii) biometric or health data, or (iv) birth date.

"Personal Information" means information provided to the Provider by or at the direction of DART or to which access was provided to the Provider at the direction of DART, in the course of the Provider's performance under this Contract that: (i) identifies or can be used to identify and individual (including and without limitation names, signatures, addresses, telephone numbers, e-mail addresses, and other unique identifiers); or (ii) can be used to authenticate an individual (including and without limitation employee identification numbers, government issued identification numbers, passwords or personal identification numbers, financial account numbers, credit report information, biometric

or health data, answers to security questions, and other personal identifiers); (iii) without limitation, all Highly Sensitive Personal Information. DART employees' business contact information is not by itself deemed to be Personal Information.

"Security Incident" means (i) any act or omission that compromises the security, confidentiality, or integrity of Personal Information, including any compromise of physical, technical, administrative, or organizational safeguards put in place by the Provider or Any Authorized Persons which relate to the security, confidentiality, or integrity of Personal Information; or (ii) receipt of a complaint in relation to the privacy practices of the Provider or any Authorized Persons; or a breach or alleged breach of this Contract relating to such privacy practices.

Terms

1. Standards of Care. The Provider agrees to abide by the following Standards of Care concerning the treatment of Personal Information:

1) Provider acknowledges and agrees that, in the course of their engagement by DART, Provider may receive or have access to Personal Information. Provider shall comply with the terms and conditions set forth in this Contract in its collection, receipt, transmission, storage, disposal, use, and disclosure of such Personal Information under its control or in its possession by All Authorized Employees and Authorized Persons. Provider shall be responsible for, and remain liable to, DART for the actions and omissions of all Authorized Persons who are not Authorized Employees concerning the treatment of Personal Information as if they were the Provider's own actions and omissions.

2) Personal Information is deemed to be the Confidential Information of DART and is not Confidential Information of the Service Provider. If in the event of a conflict or inconsistency between this section and the confidentiality/compliance with laws sections of this Contract, the terms and conditions set forth in this Section shall govern.

3) In recognition of the foregoing, Provider agrees and covenants that it shall:

   a) Keep and maintain all Personal Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access or disclosure;

   b) Use and disclose Personal Information solely and exclusively for the purposes for which the Personal information, or access to it, is provided pursuant to the terms and conditions of this Contract, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Information for the Service Provider's own purposes or for the benefit of anyone other than DART, in each case without DART's prior written consent; and

c) Not, directly nor indirectly, disclose Personal Information to any person other than the Provider's Authorized Employees/Authorized Persons including any unauthorized employees, independent contractors, subcontractors, agents, outsourcers, or auditors (an "Unauthorized Third Party"), without the express written consent from DART, unless and to the extent required by Government Authorities or as otherwise to the extent expressly required by applicable law. In such cases Provider shall (i) use best efforts to notify DART before such disclosure or as soon thereafter as reasonably possible; (ii) be responsible and remain liable to DART for the actions and omissions of such Unauthorized Third Party concerning the treatment of such Personal Information as if they were the Provider's own actions and omissions; and (iii) require the Unauthorized Third Party that has access to Personal Information to execute a written Contract agreeing to comply with the terms and conditions of this Contract relating to the treatment of Personal Information.

2. Information Security Standards. The Provider agrees to abide by the following Information Security Standards concerning the treatment of Personal Information:

1) Provider represents and warrants that its collection, access, use, storage, disposal and disclosure of Personal Information does and will comply with all applicable federal, state, and foreign privacy and data protection laws, as well as all other applicable regulations and directives.

2) Without limiting the Provider's obligations, Provider shall implement administrative, physical, and technical safeguards to protect Personal Information that are no less rigorous than accepted industry practices including specifically the International Organization for Standardization's standards: ISO/IEC 27001:2005 – Information Security Management Systems – Requirements and ISO-IEC 27002:2005 – Code of Practice for International Security Management, the Information Technology Library (ITIL) standards, the Control Objectives for Information and related Technology (COBIT) standards, or other applicable industry standards for information security; and shall ensure that all such safeguards, including the manner in which Personal Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Contract.

3) If, in the course of its engagement by DART, Provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, Service Provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the Provider's sole cost and expense.

4) At a minimum, Provider and its Authorized Persons' safeguards for the protection of Personal Information shall include: (i) limiting access of Personal Information to Authorized Employees/Authorized Persons; (ii) securing business facilities, data centers, paper files, servers, back-up systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, device application, database, and platform security; (iv) securing information transmission, storage, and disposal; (v) implementing authentication and access controls within media, applications, operating systems, and equipment; (vi) encrypting Highly-Sensitive Personal Information stored on any mobile media; (vii) encrypting Highly-Sensitive Personal Information transmitted over public or wireless networks; (viii) strictly segregating Personal Information from information of Provider or its other customers so that Personal Information is not commingled with any other types of information; (ix) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (x) providing appropriate privacy and information security training to Provider's employees.

5) During the term of each Authorized Employee's employment by the Provider, Provider shall at all times cause such Authorized Employees to abide strictly by Provider's obligations under this Contract and Provider's standard policies and procedures, a copy of which have been provided to DART. Provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use, or disclosure of Personal Information by any of Provider's officers, partners, principals, employees, agents, or subcontractors. Upon DART's written request, Provider shall promptly identify for DART in writing all Authorized Employees as of the date of such request.

6) Upon DART's written request, Provider shall provide DART with a network diagram that outlines Provider's information technology network infrastructure and all equipment used in relation to fulfilling of its obligations under this Contract, including, without limitation: (i) connectivity to DART and all third parties who may access Provider's network to the extent the network contains Personal Information; (ii) all network connections including remote access services and wireless connectivity; (iii) all access control devices (for example, firewall, packet filters, intrusion detection and access-list routers); (iv) all back-up or redundant servers; and (v) permitted access through each network connection.

7) **Data Security Incident.** The Provider agrees to abide by the following standards governing Data Security Incidents:

a. In the event a Data Security Event occurs, the Provider shall:

   i. Provide DART with the name and contact information for an employee of Provider who shall serve as DART's primary security contact and shall be

available to assist DART twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Data Security Incident.

ii. Notify DART of a Data Security Incident as soon as practicable, but no later than twenty-four (24) hours after the Provider becomes aware of it.

iii. Notify DART of any Data Security incidents by telephone at the following number: (515) 283-5020/e-mailing DART with a read receipt at it@ridedart.com and with a copy by e-mail to Provider's primary business contact at DART.

b. Immediately following Provider's notification to DART of a Data Security Incident, the parties shall coordinate with each other to investigate the Data Security Incident. Provider agrees to fully cooperate with DART in DART's handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing DART with physical access to the facilities and operations affected; (iii) facilitating interviews with Provider's employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise [reasonably] required by DART.

c. Provider shall take reasonable steps to immediately remedy any Data Security Incident and prevent any further Data Security Incidents at Provider's expense in accordance with applicable privacy rights, laws, regulations, and standards. Service Provider shall reimburse DART for actual costs incurred by DART in responding to, and mitigating damages caused by, any Data Security Incident, including all costs of notice and/or remediation.

d. Provider agrees that it shall not inform any third party of any Security Breach without first obtaining DART's prior written consent, other than to inform a complainant that the matter has been forwarded to DART's legal counsel. Further, Provider agrees that DART shall have the sole right to determine: (i) whether notice of a Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in DART's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

e. Provider agrees to fully cooperate at its own expense with DART in any litigation or other formal action deemed reasonably necessary by DART to protect its rights relating to the use, disclosure, protection, and maintenance of Personal Information.

f. In the event of any Data Security Incident, the Provider shall promptly use its best efforts to prevent a recurrence of any such Security Breach.

8) **Oversight of Security Compliance.** Upon DART's written request, to confirm Provider's compliance with this Contract, as well as any applicable laws, regulations, and industry standards, Provider grants DART or, upon DART's election, a third party on DART's behalf, permission to perform an assessment, audit, examination, or review of all controls in Provider's physical and/or technical environment in relation to all Personal Information being handled and/or services being provided to DART pursuant to this Contract. Provider shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports Personal Information for DART pursuant to this Contract. In addition, upon DART's written request, Provider shall provide DART with the results of any audit by or on behalf of Provider performed that assesses the effectiveness of Provider's information security program as relevant to the security and confidentiality of Personal Information shared during the course of this Contract.

9) **Return or Destruction of Personal Information.** At any time during the term of this Contract at DART's written request or upon the termination or expiration of this Contract for any reason, Provider shall, and shall instruct all Authorized Persons to, promptly return to DART all copies, whether in written, electronic or other form or media, of Personal Information in its possession or the possession of such Authorized Persons, or securely dispose of all such copies, and certify in writing to DART that such Personal Information has been returned to DART or disposed of securely. Provider shall comply with all reasonable directions provided by DART with respect to the return or disposal of Personal Information.

10) **Equitable Relief.** Provider acknowledges that any breach of its covenants or obligations set forth in this Section or the Provider's standard policies and procedures may cause DART irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, DART is entitled to seek equitable relief, including a restraining order, an injunctive relief, a specific performance, and any other relief that may be available from any court, in addition to any other remedy to which DART may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Contract to the contrary.

11) **Material Breach.** Provider's failure to comply with any of the provisions of this Section is a material breach of this Contract. In such event, DART may terminate the Contract in accordance with the procedures outlined in Section 10 of this Contract.

12) **Provider's Liability Insurance.** Provider shall have cyber liability insurance that provides (i) data breach and privacy crisis management, (ii) multimedia and

media liability coverage, (iii) extortion liability coverage, (iv) network security coverage, and (v) errors and omissions coverage. Coverage shall be in the minimum amount of Five Million Dollars ($5,000,000) per occurrence.