**EXHIBIT A**

# CITY OF AUSTIN DATA SECURITY STANDARDS

The requirements of this document shall remain in effect at all times while the Contract is in effect, including any renewals or extensions of the Contract term, and shall survive the expiration or termination of the Contract until such time as no Confidential Information remains in the possession or under the control of the Company.

**1. Definitions**. Capitalized terms used in this document have the meanings set forth below:

**A.** "Authorized Person" mean an employee or agent of the Company, and also means an employee or agent of a Subcontractor, who has need to know or otherwise access Confidential Information to enable the Company to perform its obligations under this Agreement, and who are bound in writing by confidentiality and other obligations sufficient to protect Personal Information in accordance with the terms and conditions of this Agreement.

**B.** "Company" means the entity that enters into the Contract with the City, and also includes all subcontractors and third parties performing any part of the Contract through or on behalf of the Company.

**C.** "Confidential Information" means electronic data (including data compilations) which is located in the System or sent to the System for storage by any User, and which concerns the City's present, past, or potential future legal affairs or legal business. By way of example and not limitation, Confidential Information includes: (1) court filings; (2) legal memoranda; (3) communications to or from a current or past member of the City Law Department; (4) files containing legal research, analysis, or other attorney work product; (5) legislative documents including, without limitation, City Council ordinances and resolutions; (6) non-public information about current or past City employees, including without limitation disciplinary documents, investigative materials, compensation information, or personal health information; (7) information related to pending, past, or threatened litigation involving the City, including without limitation demands, claims, discovery materials, expert reports, legal strategy communications, settlement materials, and similar materials; and (8) any other information that is marked or identified as confidential or would reasonably be understood to be confidential whether or not marked or identified as confidential. Confidential Information also includes Personal Information as defined in this document. "Confidential Information" remains subject to the Data Security Standards regardless of whether such data has been made public by the City or other person.

**D.** "Contract" means the agreement between the City and the Company made pursuant to City solicitation No. RFP 5700 SAP3000.

**E.** "Data Security Standards" means the physical, technical, administrative, and organizational safeguards stated in Section 2 of this document to protect the security of the System or protect Confidential Information.

**F.** "Personal Information" means data provided to the Company by or at the direction of the City, or information created or obtained by the Company on behalf of the City, that: (i) identifies or can be used to identify an individual (including, without limitation, names, addresses, telephone numbers, e-mail addresses, Social Security numbers, driver's license numbers, credit or debit card numbers, or other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, system identification numbers, passwords, PINs, answers to security questions, or other user authentication information). "Personal Information" also includes biometric, genetic, medical, or medical insurance-related data provided to the Company by or at the direction of the City under the Contract.

**G.** "Security Breach" means: (i) any breach of the Data Security Protections that results in unauthorized access by any person to Confidential Information; (ii) any act or omission that compromises the Data Security Protections and results in potential unauthorized access by any person to Confidential Information; (iii) receipt by the City or the Company of notice from any third party alleging a breach of the Data Security Protections resulting in unauthorized access to such third party's confidential information.

**H.** "System" means all of the Company's matter management software application(s) deployed to meet the City's needs under the Contract, and also includes all hardware, network connections, data storage, third party applications, and other elements owned by or used by the Company to perform the Contract.

**2. <u>Data Security Standards</u>.**

**A.** The Company shall comply with all Data Security Standards so long as the Contract is in effect (including any option periods or extensions of the Contract), and for any such additional period of time that the Company has Confidential Information in its possession or under its control. The Company shall be responsible for compliance with these Data Security Standards by all Authorized Persons.

**B.** The Company shall:

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

(2) Not create, collect, receive, access, or use Confidential Information in violation of applicable law;

(3) Use and disclose Confidential Information solely and exclusively for the purposes for which such information, or access to it, is provided pursuant to the terms of the Contract, and shall not use, sell, rent, transfer, distribute, or otherwise disclose or make available Confidential Information for the Company's own purposes or for the benefit of anyone other than the City without the City's prior written consent; and

(4) Not directly or indirectly disclose Confidential Information to any person other than Authorized Persons without the City's prior written consent.

**C.** The Company shall implement and maintain a written information security program, including appropriate policies, procedures, and risk assessments that are reviewed and updated at least annually.

**D.** The Company shall store and process all Confidential Information within the contiguous United States.

**E.** The Company shall implement administrative, physical, and technical safeguards to protect Confidential Information from unauthorized access, acquisition, disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than the National Institute of Standards and Technology ("NIST") Cybersecurity Framework standards and shall ensure that all such safeguards, including the manner in which Personal Information is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Agreement. At a minimum, such safeguards shall include:

(1) Limiting access to Confidential Information to Authorized Persons such that Authorized Persons have only the minimum level of access required to perform the Company's obligations under this Agreement;

(2) Securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability;

(3) Implementing network, application, database, and platform security;

(4) Securing information transmission, storage, and disposal;

(5) Implementing authentication and access controls within media, applications, operating systems, and equipment;

(6) Encrypting all Confidential Information during storage on any media and at all times while in transit over public or wireless networks;

(7) Strictly segregating Confidential Information from other information held by the Company such that Confidential Information is not commingled with any other types of data;

(8) Conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing at the Company's sole cost and expense corrective action plans to correct any issues reported as a result of the testing;

(9) Implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law;

(10) Providing appropriate privacy and information security training to Authorized Persons;

(11) Prohibiting endpoint storage.

**F.** The Company shall, at all times, cause Authorized Persons to abide strictly by the Company's obligations under this Agreement. The Company further agrees that it shall maintain a disciplinary/sanctions process to address any unauthorized access, use, or disclosure of Confidential Information by any Authorized Person. Upon the City's written request, the Company shall promptly identify for the City, in writing, all Authorized Persons as of the date of such request.

**G.** Upon the City's written request, the Company shall provide the City with a network diagram that outlines the Company's information technology network infrastructure and all equipment used in relation to fulfilling its obligations under this Agreement, including, without limitation: (i) connectivity to the City and all third parties who may access the Company's network to the extent the network contains Confidential Information; (ii) all network connections, including remote access services and wireless connectivity; (iii) all access control measures (for example, firewalls, packet filters, intrusion detection and prevention services, and access-list-controlled routers); (iv) all backup or redundant servers; and (v) permitted access through each network connection.

**H. Security Breach Procedures.**

(1) In the event of a Security Breach the Company shall:

a. Provide the City with the name and contact information for an employee of the Company who shall serve as the City's primary security contact and who shall be available to assist the City twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Breach; and

b. Notify the City of a Security Breach as soon as practicable, but no later than four hours after the Company becomes aware of such breach, as follows:

i. To the City's Communications and Technology Management Department by telephone (512-974-4357) and e-mail (cybersecurity@austintexas.gov); and

ii. To the City Attorney by telephone (512-974-2268) and fax transmission (512-974-2894).

c. Notice sent by email and fax transmission under this subsection (b) shall include:

i. A description of type, size, and scope of the Security Breach;

ii. A description of the actions taken by the Company to remedy the Security Breach;

iii. A statement of whether the Security Breach has been resolved or is ongoing; and

iv. contact information for the Company representative(s) available to the City to communicate about the Security Breach.

(2) Immediately following the Company's notification to the City of a Security Breach, the Parties shall coordinate with each other to investigate the Security Breach. If the Security Breach results in the disclosure of Confidential Information, the City will notify affected persons and may notify the Texas Attorney General in accordance with Texas Business and Commerce Code § 521.053. The Company agrees to fully cooperate with the City in the City's handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing the City with physical access to the facilities and operations affected; (iii) facilitating interviews between the City and the Company's employees, Authorized Persons, 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 required by the City.

(3) The Company shall, at its own expense, use best efforts to immediately contain and remedy any Security Breach and prevent any further Security Breach, including, but not limited to, taking any and all action necessary to comply with applicable privacy rights, laws, regulations, and standards. The Company shall reimburse the City for all actual costs incurred by the City in responding to, and mitigating damages caused by, any Security Breach, including all costs of notice and/or remediation.

(4) The Company agrees that it shall not inform any third party of any Security Breach without first obtaining the City's prior written consent. Further, the Company agrees that the City shall have the sole right to determine: (i) whether notice of the 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 the City'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.

(5) The Company agrees to maintain and preserve all documents, records, and other data related to any Security Breach.

(6) The Company agrees to fully cooperate, at its own expense, with the City in any litigation, investigation, or other action deemed necessary by the City to protect its rights relating to the use, disclosure, protection, and maintenance of Personal Information.

**I. Oversight of Security Compliance.** On written request from the City, the Company shall permit the City (or third party designated by the City) to perform an assessment, audit, examination, or review of all controls in the Company's physical and/or technical environment in relation to all Confidential Information. The Company shall fully cooperate

with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports Confidential Information for the City pursuant to this Agreement. In addition, upon the City's written request, the Company shall provide the City with the results of any audit performed by or on behalf of the Company that assesses the effectiveness of the Company's information security program as relevant to the security of Confidential Information.

**J.** **Return or Destruction of Personal Information**. On written request at any time during the term of the Contract, or at the termination or expiration of the Contract for any reason, the Company shall, and shall instruct all Authorized Persons to, promptly return to the City all Confidential Information (whether in written, electronic, or other form or media) in its possession or the possession of such Authorized Persons. The Parties may alternatively agree that the Company may dispose of some or all parts of the Confidential Information the Company holds and certify in writing to the City that such Confidential Information has been disposed of securely. The Company shall comply with all directions provided by the City with respect to the return or disposal of Confidential Information.

**K.** **Equitable Relief**: The Company acknowledges that any breach of its covenants or obligations set forth in this Section may cause the City irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the City is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance, and any other relief that may be available from any court, in addition to any other remedy to which the City 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, notwithstanding any exclusionsor limitations in this Agreement to the contrary.