MASTER INTERLOCAL AGREEMENT No. UTA19-000382
BETWEEN
THE CITY OF AUSTIN, TEXAS
AND
THE UNIVERSITY OF TEXAS AT AUSTIN
FOR
RESEARCH, CONSULTING, AND TECHNICAL ASSISTANCE

THIS MASTER INTERLOCAL AGREEMENT ("Master Agreement") is entered into and effective the **1st** day of October, 2020, by and between the City of Austin, a home-rule municipality incorporated under the law of the State of Texas (the "City"), and the University of Texas at Austin, an institution of higher education and agency of the State of Texas (the "University") (hereinafter each referred to individually as a "Party" and collectively as the "Parties"), acting by and through their respective governing bodies, pursuant to and under authority of the Interlocal Cooperation Act, Chapter 791 of the Texas Government Code.

RECITALS:

WHEREAS, this Master Agreement is authorized by Chapter 791 of the Texas Gov't Code; and

WHEREAS, the City is a local government entity as that term is defined in Tex. Gov't Code Sec. 791.003 and the University is an institution of higher education and part of a university system as defined in Tex. Gov't Code Sec. 791.035 and Tex. Edu. Code Sec. 61.003; and

WHEREAS, the University is considered by the City to be qualified to conduct research projects (the "Projects") on the performance of the City's governmental functions, so as to allow the City to identify innovative solutions for serving City residents and addressing local challenges; and

WHEREAS, the City desires to engage the University to conduct the Projects; and

WHEREAS, the research will be focused on the performance of governmental functions or services as that is defined in Tex. Gov't Code Sec. 791.003(3); and

WHEREAS, the City and the University anticipate working together on a range of governmental functions or service Projects over the period governed by the Master Agreement; and

WHEREAS, payment under the Master Agreement will be made based on a cost-recovery method, and therefore the Projects are not subject to competitive procurement under Tex. Gov't Code Sec. 791.035; and

WHEREAS, the Projects will help the City to achieve its Strategic Directions 2023 goals in the categories of Mobility, Safety, Health and Environment, Culture and Lifelong Learning, Government that Works for All, and Economic Opportunity and Affordability; and

WHEREAS, both Parties desire to enter into this Master Agreement to outline common terms and streamline the process of researching the performance of the City's governmental functions, so as to promote innovation, develop new insights, and otherwise assess how the City can best carry out the performance of governmental functions in the 21st century;

NOW THEREFORE, it is agreed between the Parties hereto that:

AGREEMENT

ARTICLE I
PURPOSE

The purpose of this Master Agreement is to establish pre-negotiated terms and conditions, as well as a framework for research, consulting, and technical services to be exchanged between the University and the City.

ARTICLE II
CITY RESPONSIBILITIES

(i) The City will initiate each Project via a Work Order as provided in Article IV.

(ii) The City agrees to provide data as needed to conduct each Project. The City shall have the sole discretion to determine what City data will be shared with the University for the purpose of each Project.

(iii) The City may make staff available to assist with the data sharing and other work required for each Project.

ARTICLE III
UNIVERSITY RESPONSIBILITIES

The University shall provide Projects to the City pursuant to the terms of this Master Agreement. The Projects may include, but are not limited to:

(i) academic research involving University faculty, staff, or students;
(ii) community-based research;
(iii) program evaluation;
(iv) best practice studies;
(v) strategic planning assistance;
(vi) data analysis;
(vii) survey research; and
(viii) use of City departments / services / data for academic research by faculty or students.

The University will administer the Services in a manner satisfactory to the City and consistent with any standards required under the terms and conditions of this Master Agreement, or any special conditions required by any City funding source as set forth in the Work Order (as defined below) and mutually agreed upon by the Parties.

The University agrees that any non-exempt human and/or vertebrate animal research protocol conducted under this Master Agreement shall be reviewed and approved by the appropriate Institutional Review Board (IRB) and/or its Institutional Animal Care and Use Committee (IACUC), as applicable, and that it will follow current and duly approved research protocols for all periods of the applicable Work Order involving human and/or vertebrate animal research. University certifies that its IRB and/or IACUC are in full compliance with applicable state and federal laws and regulations. University certifies that any submitted IRB/IACUC approval represents a valid, approved protocol that is entirely consistent with the project associated with the applicable Work Order. In no event shall the University invoice or be reimbursed for any human or vertebrate animals related research expenses incurred in a period where any applicable IRB/IACUC approval is not properly in place.

ARTICLE IV
WORK ORDERS

The City shall initiate each Project with the University by providing the University with a "Work Order" in the format attached to this Master Agreement as **Exhibit A**. The compensation under this Master Agreement shall not exceed one million five-hundred thousand dollars ($1,500,000) per year, and the total compensation under this Master Agreement shall not exceed seven million five-hundred thousand dollars ($7,500,000). The Parties must both agree to and sign a Work Order before commencing a Project described in a Work Order.

Each Work Order shall include, at a minimum:

(i) Project title and a description of the Projects to be performed, including any deliverables;
(ii) Identification of relevant City and University Departments, a principal investigator, and points of contact from the City and the University;
(iii) The cost of the Projects performed, including a detailed Project budget if required;
(iv) The period of performance of the Work Order;
(v) Invoicing Instructions;
(vi) Description of any data to be shared;
(vii) The University's determination of whether IRB review and approval are required;
(viii) Special terms and conditions, including reporting requirements; and
(ix) Any other information required to carry out the Work Order.

The City and the University may collaborate on pursuing federal, state, local, and private grant funding for any project to be covered by a Work Order under this Master Agreement. However,

the City's acceptance, commitments, obligations or expenditures toward a grant purpose must be approved in accordance with City Administrative Bulletin 08-04.

Any alterations, variations, modifications, or waivers of provisions of an approved Work Order shall be made in writing executed by the authorized signatories of both Parties to that Work Order. If there is any conflict between the terms of the Master Agreement and a Work Order, the terms of this Master Agreement shall prevail.

ARTICLE V
TERM AND COMMENCEMENT

The term of this Master Agreement commences on October 1, 2020 and shall continue in full force and effect through October 1, 2025, unless terminated prior to expiration.

ARTICLE VI
TERMINATION AND DISPUTE RESOLUTION

a. **Default.** A Party shall be in default under this Agreement if the Party fails to fully, timely, and faithfully perform any of its material obligations under this Agreement, and following receipt of written notice of such failure fails to timely cure the failure within thirty (30) business days.

b. **Termination for Cause.** In the event of a default by a Party, the other Party will have the right to terminate the Agreement for cause, by written notice delivered by certified mail to the Party in default. Unless the Party giving notice specifies a different time in the notice, the Agreement is terminated thirty (30) calendar days after the date of the notice. During this time period, the Party alleged to be in default may cure the default or provide evidence sufficient to prove to the other party's reasonable satisfaction that the default does not exist or will be cured in a time satisfactory to the Party alleging default. In addition to any other remedy available under law or in equity, the Party not in default shall be entitled to recover all actual damages and direct costs incurred as a result of the other Party's default, and prejudgment and post-judgment interest at the maximum lawful rate. Each Party's rights and remedies under the Agreement are cumulative and are not exclusive of any other right or remedy provided by law.

c. **Termination for Convenience.** This Master Agreement may be terminated by either Party by giving ninety (90) days' written notice to the other Party of its intention to terminate. Work Orders executed by both Parties will continue in effect unless one Party provides the other with thirty (30) days' advance notice, in writing, of its intention to terminate.

d. **Dispute Resolution.** If a dispute arises between the Parties regarding performance under this Agreement, which the Parties are unable to resolve through negotiation, the Parties agree that the dispute will be submitted for mediation before any suit is filed. If mediation does not successfully resolve the dispute, each Party is free to pursue other remedies available to them.

ARTICLE VII
INVOICES AND PAYMENT

a. **Invoices**

i. The City agrees to pay the University the amount invoiced, with the understanding that the University will maintain and provide all documents, receipts, timesheets, invoices and other information to show salary and other expenses, as requested.

ii. The University shall submit monthly or quarterly cost-incurred invoices for work completed in accordance with the scheduled milestones and objectives listed in each Work Order.

iii. Proper Invoices must include a unique invoice number, the Work Order number and the master agreement number if applicable, the Department's Name, and the name of the point of contact for the Department. Invoices shall be itemized.

iv. The University must submit invoices which include documentation of names of graduate students, level of effort, description of work performed, and any related expenses/costs associated with the Project. Each invoice must have a unique invoice number.

v. Unless otherwise expressly authorized in the Contract, the Contractor shall pass through all subcontract and other authorized expenses at actual cost without markup.

vi. Invoices will include appropriately charged indirect costs, following the University's active indirect cost rate agreement and associated policy.

vii. Federal excise taxes, State taxes, or City sales taxes must not be included in the invoiced amount. The City will furnish a tax exemption certificate upon request.

b. **Payment**

i. All proper invoices received by the City will be paid within thirty (30) calendar days of the City's receipt of the invoice, provided University has met required milestones to date.

ii. If payment is not timely made, interest shall accrue on the unpaid balance at the lesser of the rate specified in Texas Government Code Section 2251.025 or the maximum lawful rate; except, if payment is not timely made for a reason for which the City may withhold payment hereunder, interest shall not accrue until ten (10) calendar days after the grounds for withholding payment have been resolved.

iii. Notice is hereby given of Article VIII, Section 1 of the Austin City Charter which prohibits the payment of any money to any person, firm or corporation who

is in arrears to the City for taxes, and of §2-8-3 of the Austin City Code concerning the right of the City to offset indebtedness owed the City.

iv. Payment will be made by electronic transfer of funds. The University agrees that there shall be no additional charges, surcharges, or penalties to the City for payments made by credit card or electronic funds transfer.

v. The City's payment obligations are payable only and solely from funds appropriated and available for this Master Agreement and each Work Order. The absence of appropriated or other lawfully available funds shall render the Master Agreement and affected Work Orders null and void to the extent funds are not appropriated or available. The City shall provide the University written notice of the failure of the City to make an adequate appropriation for any fiscal year to pay the amounts due under the Master Agreement or Work Order, or the reduction of any appropriation to an amount insufficient to permit the City to pay its obligations under the Master Agreement or Work Order. In the event of non or inadequate appropriation of funds, there will be no penalty nor removal fees charged to the City, however University will be paid for work performed prior to termination or non-appropriation.

vi. Payments should be made to the University of Texas at Austin, and submitted to the following address:

The University of Texas at Austin
Office of Accounting
P.O. Box 7159
Austin, Texas 78713-7159
(512) 471-6231

vii. Project costs shall not exceed the costs identified in the Project's Work Order unless mutually agreed upon in a writing signed by both Parties. Prior to requesting funding above the amount allotted in the Work Order, the University shall provide a preliminary report or analysis of the Project results to the City.

ARTICLE VIII
FISCAL FUNDING

The financial obligations of the Parties, if any, under this Master Agreement are contingent upon the availability and appropriation of sufficient funding. Each Party paying under this Master Agreement must make those payments from current revenues available to the paying Party. Any Party may withdraw from this Master Agreement without penalty in the event that funds are not available or appropriated. However, no Party will be entitled to a refund of amounts previously contributed in the event of withdrawal for lack of funding.

ARTICLE IX
SELF-INSURANCE

Each Party is self-insured and therefore an insurance policy is not required. Each Party will provide proof of self-insurance upon request. To the extent allowed by Texas law, each Party agrees to be responsible for its own proportionate share of liability for its negligent acts and omissions for claims, suits, and causes of action, including claims for property damage, personal injury, and death, arising out of or connected to this Master Agreement and as determined by a court of competent jurisdiction, provided that the execution of this Master Agreement, and related Work Orders, will not be deemed a negligent act.

ARTICLE X
NO ENDORSEMENT

In no event shall either Party state or imply in any publication, advertisement, or other medium that the other Party has approved, endorsed, or tested any Project. In no event shall the Parties' performance of the scope of Projects described in Section II be considered the basis for any endorsement of a product or service. Notwithstanding the foregoing, the Parties may publicly release any materials related to the Projects, including, but not limited to, the report, faculty or employee names, research methodology, recommendations, and other items that do not expressly state that the other Party endorses the Services.

ARTICLE XI
USE OF NAME OR LOGO

Each Party agrees not to use the name, logo, or any other marks (including, but not limited to, colors and music) owned by or associated with the other Party or the name of any representative of the other Party in any sales promotion work or advertising, or any form of publicity, without the prior written permission of the other Party in each instance. Nothing in the foregoing restricts the Parties' right to publicly release any reports or documents generated as part of the Project, including any name, logo, or other marks contained within such documents. The Parties may amend the restrictions of this clause in an approved Work Order.

ARTICLE XII
PUBLICATIONS AND DISTRIBUTIONS

The University may publish or otherwise disseminate the research result from any work undertaken pursuant to a Work Order. The University will provide co-author credit to City staff where City staff co-author any written work for publication. University will provide appropriate acknowledgement of City funding for the project and will provide to the City a copy of the manuscript or presentation first disseminating the research results for the City's review at least thirty (30) days prior to publication or presentation. University will consider the City's comments and suggested modifications.

ARTICLE XIII
OWNERSHIP AND USE OF INTELLECTUAL PROPERTY

All intellectual property developed prior to, or outside, this Master Agreement ("Background Intellectual Property") and disclosed in connection with a Work Order initiated under this Master Agreement shall remain the exclusive property of the Party introducing and/or disclosing such Background Intellectual Property to the other Party. The Parties agree that the use of such Background Intellectual Property for purposes under this Master Agreement does not constitute permission, whether implied or otherwise, to use the aforementioned Background Intellectual Property for any purpose beyond the scope of an applicable Work Order.

All intellectual property, including copyrightable works and patentable inventions, developed under this Master Agreement ("Foreground Intellectual Property") shall be owned by the Party or Parties whose employees develop such Foreground Intellectual Property. For the avoidance of doubt, title to all Foreground Intellectual Property made solely by University under this Master Agreement shall reside in University, title to all Foreground Intellectual Property made solely by City shall reside in City, and title to all Foreground Intellectual Property made jointly by University and City shall reside jointly in University and City.

The University hereby licenses and grants to the City a permanent, irrevocable, nonexclusive, non-commercial, and royalty-free license to use, reproduce, copy, publish, prepare derivative works from, distribute to the public, perform, and display publicly for or on behalf of the City, the intellectual property rights in the copyrightable deliverables developed as part of the work under this Master Agreement. The University agrees to grant to the City a nonexclusive, royalty-free license to use all patentable inventions developed by University under this Master Agreement for the City's non-commercial, internal, governmental purposes.

The University hereby certifies that it will not knowingly infringe on any third-party copyright ownership in the conduct of work under this Master Agreement.

ARTICLE XIV
TEXAS PUBLIC INFORMATION ACT

Each Party acknowledges that they are subject to the Texas Public Information Act, currently codified under Texas Government Code Chapter 552.

ARTICLE XV
CONFIDENTIALITY

The Parties may be granted access to certain of the other Party's or licensor's confidential information or data (including inventions, employee information, confidential know-how, confidential business information, and other information which the Parties or their licensors consider confidential) ("Confidential Information") to provide the Projects to the City. Confidential Information will be transmitted in writing and clearly marked "Confidential," "Proprietary," or similarly, or if disclosed orally will be reduced to writing by disclosing Party, clearly marked "Confidential," "Proprietary," or similarly, and transmitted to the receiving Party

within thirty (30) days after oral disclosure. The Parties acknowledge and agree that the Confidential Information is the valuable property of the disclosing Party and its licensors and any unauthorized use, disclosure, dissemination, or other release of the Confidential Information will substantially injure the non-disclosing Party and its licensors. The Parties (including their employees, Subcontractors, agents, or representatives) agree to maintain the Confidential Information in strict confidence and shall not disclose, disseminate, copy, divulge, recreate, or otherwise use the Confidential Information without the prior written consent of the disclosing Party, or in a manner not expressly permitted under this Master Agreement, unless the Confidential Information is required to be disclosed by law or an order of a court or other governmental authority (including a Texas Attorney General Opinion) with proper jurisdiction. In all cases, the Parties agree to promptly notify the disclosing Party before disclosing Confidential Information to permit the disclosing Party reasonable time to seek an appropriate protective order. The Parties agree to use protective measures no less stringent than the Parties use in their own business to protect their own most valuable information. In all circumstances, the Parties' protective measures must be at least reasonable measures to ensure the continued confidentiality of the Confidential Information.

A. The Parties agree: (i) not to use Confidential Information for any reason other than for the purpose of providing or receiving the Projects, (ii) not to disclose Confidential Information to any third party other than to each Party's employees subrecipients, and subcontractors who have a need to know the Confidential Information for furtherance of providing the Projects, (iii) to promptly notify the disclosing Party of any request for Confidential Information to be disclosed under any law or order of any court or other governmental authority with proper jurisdiction, so as to permit the disclosing Party reasonable time to seek an appropriate protective order, and (iv) to use measures to protect the Confidential Information that are no less stringent than the Party uses within its own entity to protect its own most valuable information, which protective measures shall under all circumstances be at least reasonable measures to ensure the continued confidentiality of the Confidential Information.

B. All Confidential Information and derivations thereof shall remain the sole and exclusive property of disclosing Party, and no license or other right to the Confidential Information or intellectual property is granted or implied hereby. Upon the written request of the disclosing Party, the non-disclosing Party shall promptly return to the disclosing Party all tangible items of Confidential Information furnished by disclosing Party and all copies thereof or certify in writing that all Confidential Information, including all copies, has been destroyed.

C. No expiration or termination of the Master Agreement shall affect either Party's rights or obligations with respect to Confidential Information.

D. The Parties acknowledge and agree that any breach or threatened breach of the Master Agreement could cause harm for which money damages may not provide an adequate remedy. The Parties agree that in the event of such a breach or threatened breach of the Master Agreement, in addition to any other available

remedies, the disclosing Party may seek temporary and permanent injunctive relief restraining the non-disclosing Party from disclosing or using, in whole or in part, any Confidential Information.

ARTICLE XVI
DATA SECURITY

In the course of providing services to the City, the University may gain access to City-owned and City-maintained information or data. If so, the City and the University desire to keep such information appropriately protected. The University will handle information it receives from Austin Energy in compliance with the Austin Energy Data Handling Controls, attached as **Exhibit B** to this Agreement. The University will handle all other information it receives from the City in compliance with this provision.

A. **Definitions**. Capitalized terms used in this Section shall have the meanings set forth below:

(1) "Authorized Persons" mean (i) the University's employees; and (ii) the University's Subcontractors and agents who have a need to know or otherwise access Personal Information to enable the University to perform its obligations under this Master 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 Master Agreement.

(2) "Highly Sensitive Personal Information" means an (i) individual's government-issued identification number (including Social Security number, driver's license number, or State-issued identification number); (ii) financial account number, credit card number, debit card number, or 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; or (iii) biometric, genetic, health, medical, or medical insurance data.

(3) "Personal Information" means information or data provided to the University by or at the direction of the City, information which is created or obtained by the University on behalf of the City, or information to which access was provided to the University by or at the direction of the City, in the course of the University's performance under this Master Agreement that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses, and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, user identification and account access credentials or passwords, financial account numbers, credit report information, student information, biometric, health, genetic, medical, or medical insurance data, answers to security questions, and other personal identifiers), in case of both

subclauses (i) and (ii), including, without limitation, all Highly Sensitive Personal Information.

(4) "Public Information" has the same meaning as "public information" as defined in Chapter 552 of the Texas Government Code.

(5) "Security Breach" means (i) any act or omission that compromises either the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards put in place by the University or any Authorized Persons, or by the City should the University have access to the City's systems, that relate to the protection of the security, confidentiality, or integrity of Personal Information, or (ii) receipt of a complaint in relation to the privacy and data security practices of the University or any Authorized Persons or a breach or alleged breach of this Master Agreement relating to such privacy and data security practices. Without limiting the foregoing, a compromise shall include any unauthorized access to or disclosure or acquisition of Personal Information.

B. **Standard of Care**:

(1) The University acknowledges and agrees that, during the term of this Master Agreement, the University may create, receive, or have access to Personal Information. For any Personal Information, the University shall comply with this Section in its creation, collection, receipt, transmission, storage, disposal, use, and disclosure of such Personal Information and be responsible for any unauthorized creation, collection, receipt, transmission, access, storage, disposal, use, or disclosure of Personal Information under its control or in its possession by all Authorized Persons. The University shall be responsible for, and shall remain liable to, the City for the actions and omissions of all Authorized Persons concerning the treatment of Personal Information.

(2) Personal Information is deemed to be Confidential Information of the City and is not Confidential Information of the University. In the event of a conflict or inconsistency between this Section and any other section of this Master Agreement, the terms and conditions of this Section shall govern and control.

(3) The University 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, use, or disclosure;
b. Not create, collect, receive, access, or use Personal Information in violation of law;

c. 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 Master Agreement, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Information for the University's own purposes or for the benefit of anyone other than the City, in each case, without the City's prior written consent; and
d. Not, directly or indirectly, disclose Personal Information to any person other than Authorized Persons, without the City's prior written consent.

(4) The University represents and warrants that its creation, collection, receipt, access, use, storage, disposal, and disclosure of Personal Information does and shall comply with all applicable Federal and State privacy and data protection laws, as well as all other applicable regulations and directives.

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

The University shall store and process all Personal Information within the contiguous United States.

Without limiting the University's obligations under this Section, the University shall implement administrative, physical, and technical safeguards to protect Personal Information from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than the National Institute of Standards and Technology ("NIST") Cybersecurity Framework 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 Master Agreement.

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

(6) At a minimum, the University's safeguards for the protection of Personal Information shall include: (i) limiting access of Personal Information to Authorized Persons, so that Authorized Persons have only the minimum

level of access required to perform the University's obligations under this Agreement; (ii) 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; (iii) implementing network, 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 media; (vii) encrypting Highly Sensitive Personal Information transmitted over public or wireless networks; (viii) strictly segregating Personal Information from information of the University or its other customers so that Personal Information is not commingled with any other types of information; (ix) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at the University's sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing; (x) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; (xi) providing appropriate privacy and information security training to Authorized Persons; and (xii) prohibiting endpoint storage.

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

(8) Upon the City's written request, the University shall provide the City with a network diagram that outlines the University's information technology network infrastructure and all equipment used in relation to fulfilling its obligations under this Master Agreement, including, without limitation: (i) connectivity to the City and all third parties who may access the University'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 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.

C. **Security Breach Procedures**:

(1) The University shall:

a. Provide the City with the name and contact information for an employee of the University 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;

b. Notify the City of a Security Breach as soon as practicable, but no later than twenty-four (24) hours after the University becomes aware of it; and

c. Notify the City (CTM Service Desk) of any Security Breaches by telephone at 512-974-4357 and e-mail at cybersecurity@austintexas.gov.

(2) Immediately following the University'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 Highly Sensitive Personal 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 University 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 University'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 University 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 University 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 University agrees that it shall not inform any third party of any Security Breach without first obtaining the City's prior written consent. Further, the University 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 University agrees to maintain and preserve all documents, records, and other data related to any Security Breach.

(6) The University 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.

(7) In the event of any Security Breach, the University shall promptly use its best efforts to prevent a recurrence of any such Security Breach.

D. **Oversight of Security Compliance**:
Upon the City's written request to confirm the University's compliance with this Master Agreement, as well as any applicable laws, regulations, and industry standards, the University grants the City or, upon the City's election, a third party on the City's behalf, permission to perform an assessment, audit, examination, or review of all controls in the University's physical and/or technical environment in relation to all Personal Information being handled and/or services being provided to the City under this Master Agreement. The University 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 the City pursuant to this Master Agreement. In addition, upon the City's written request, the University shall provide the City with the results of any audit performed by or on behalf of the University that assesses the effectiveness of the University's information security program as relevant to the security and confidentiality of Personal Information shared during the course of this Master Agreement.

E. **Return or Destruction of Personal Information**: At any time during the term of this Master Agreement, at the City's written request or upon the termination or expiration of this Master Agreement for any reason, the University shall, and shall instruct all Authorized Persons to, promptly return to the City 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 the City that such Personal Information has been returned to the City or disposed of securely. The University shall comply with all directions provided by the City with respect to the return or disposal of Personal Information.

F. **Equitable Relief**: The University 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 exclusions or limitations in this Master Agreement to the contrary.

G. **Remediation**: As soon as practicable, and at no additional cost to the City, the University will remedy the source of the Security Incident, as required by the remediation plan. The University shall reimburse the City for all costs to City associated with the Security Incident.

H. **Recovery**: Within seven days of completing the remediation plan, the University must provide the City reasonable written assurance declaring full system recovery, signed by an executive with proper authority, attesting that the Security Incident is remediated and shall not recur.

ARTICLE XVII
NOTICES

The Parties may make routine communications by e-mail, first-class mail, telephone, or other commercially accepted means. When this Master Agreement requires the Parties to provide notice to each other, notice shall be in writing and must be addressed, hand-delivered, or e-mailed to the person designated for receipt of notice.

A mailed notice shall be considered delivered three (3) business days after postmarked if sent by U.S. Postal Service Certified or Registered Mail, Return Receipt Requested, postage prepaid. Hand-delivered notices are considered delivered only when the addressee receives those notices. Notices delivered by e-mail are considered delivered three (3) business days after transmittal or when received by the addressee, whichever is earlier.

Notice and routine communications concerning this Master Agreement shall be directed to the following Master Agreement representatives. Either Party may designate an alternative addressee, address, or other contact information by notifying the other Party in writing.

UNIVERSITY

Renee Gonzales
AVP & Director, Office of Sponsored Projects
3925 West Braker Lane, Suite 3.340
Austin, Texas, 78759
Phone: 512-471-6424
Email: osp@austin.utexas.edu

CITY

Contract Manager:
City of Austin
Kerry O'Connor, Chief Innovation Officer

301 W. 2nd Street, 3rd Floor
Austin, Texas 78701
Phone: 512-974-1637
Email: Kerry.Oconnor@austintexas.gov

Project Lead:
City of Austin
Attention: Charles Purma
Communications & Technology Management Department
1124 S. IH-35, Ste. 300
Austin, Texas 78704
Phone: 512-974-1644
Email: Charles.PurmaIII@austintexas.gov

ARTICLE XVIII
CITY'S RIGHT TO AUDIT

The University agrees that the representatives of the Office of the City Auditor or other authorized representatives of the City shall have access to, and the right to audit, examine, or reproduce, any and all such records of the University related to performance under this Agreement at the City's expense. The University agrees to refund to the City any overpayments disclosed by any such audit. The City agrees to protect from disclosure the University's confidential and proprietary information disclosed during an audit to the same extent it protects its own confidential and proprietary information, subject to the requirements of the Texas Public Information Act.

ARTICLE XIX
AMENDMENTS

This Master Agreement may be amended only by the mutual written agreement of the Parties. Neither any representation or promise made after the execution of this Master Agreement, nor any modification or amendment of this Agreement, shall be binding on the Parties unless made in writing and properly executed by each of the Parties. No pre-printed or similar terms on any invoice, Work Order, clickwrap agreement, or other document shall have any force or effect to change the terms, covenants, and conditions of the Agreement.

ARTICLE XX
NO THIRD-PARTY RIGHTS

Nothing in this Master Agreement, express or implied, is intended to confer upon any person or entity, other than the Parties hereto, any benefits, rights, or remedies under or by reason of this Master Agreement.

ARTICLE XXI
ADDITIONAL AGREEMENTS

The Parties agree to execute such other and further instruments and documents, including Work Orders, as are or may become necessary or convenient to carry out the purposes of this Master Agreement.

ARTICLE XXII
NO ASSIGNMENT

The Parties may not assign or transfer their rights under this Master Agreement.

ARTICLE XXIII
NO WAIVER OF RIGHTS

Nothing in this Master Agreement shall be deemed to waive, modify, or amend any legal defense available to a Party at law or in equity, including the defense of sovereign or governmental immunity, nor to create any legal rights or claims on behalf of a person not a party to this Master Agreement.

ARTICLE XXIV
APPLICABLE LAW

This Master Agreement shall be construed under the laws of the State of Texas. Any suits relating to this Agreement will be filed in a district court or federal court in Travis County, Texas.

ARTICLE XXV
SEVERABILITY

If a court of competent jurisdiction determines that a term or provision of this Agreement is void or unenforceable, the remainder of this Master Agreement remains effective to the extent permitted by law.

ARTICLE XXVI
ENTIRE AGREEMENT

This is the complete and entire Master Agreement between the Parties with respect to the matters herein and supersedes all prior negotiations, agreements, representations, and understandings, if any. This Master Agreement may not be modified, discharged, or changed in any respect whatsoever except by further agreement in writing and approved by both Parties.

Exhibits:

I. Exhibit A (Work Order Template)
II. Exhibit B (Austin Energy Data Handling Controls)

IN WITNESS WHEREOF, the University and the City have caused this Master Agreement to be executed on their behalf respectively by their proper officers as follows:

FOR THE UNIVERSITY:

DocuSigned by:
By: Renee Gonzales
A925A640897F493...
Name: Renée Gonzales
Title: Assistant Vice President for Research & Director, Office of Sponsored Projects
Date: 2020-09-21 | 16:03:12 PDT

FOR THE CITY:

DocuSigned by:
By: Nuria Rivera-Vandermyde
7B5ADCA8B9B04F2...
Name: Nuria Rivera-Vandermyde
Title: Deputy City Manager
Date: 2020-09-23 | 07:03:55 PDT

Approved as to Form:

DocuSigned by:
By: Holly Heinrich
E6E7935E90FA4F4...
Name: Holly Heinrich
Title: Assistant City Attorney
Date: 2020-09-22 | 07:12:41 PDT

Exhibit A

Work Order No. _____

Under Master Agreement No. UTA19-000382

[Project Name/Title]

[Lead City Department] and [Lead University Department]

Purpose

This proposed study will … [fill in purpose of study/research project].

Background

Project Timeline

This Work Order shall be effective as of the date of last signature and shall remain in effect until _____.

Statement of Work (Please include the questions to be researched)

Project Deliverables

University agrees to complete and submit the following deliverables:

Deliverable Name: Due Date:

Budget (not to exceed $XXX)

Period of Performance	_____ Months
Budget Category	**Amount**
Total Direct Costs*	
Personnel / Salary	
Travel	
Materials & Supplies	
Equipment	
Consultants / Services	
Other	
Total Indirect Costs**	
Total Cost Estimate	

***Direct Costs** (e.g. salary, fringe benefits, project-specific equipment, consultants, subcontracts, and materials and supplies) can be identified specifically with a particular final cost objective or can be directly assigned to such activities relatively easily with a high degree of accuracy. Costs incurred for the same purpose in like circumstances must be treated consistently as either direct or indirect (F&A) costs.

****Indirect (Facilities and Administrative – F&A) Costs** means those costs incurred for a common or joint purpose benefitting more than one cost objective, and not readily assignable to the cost objectives specifically benefitted. These costs include building depreciation, general purpose equipment and capital improvement, utilities, custodial services, general administration, research administration, the libraries, accounting, and purchasing.

Funding Source	Department - Unit - Object Code	Finance Contact name	
FDU		Phone #	
		Email	

Invoicing Instructions

In accordance with the terms of the Master Agreement, the University shall submit monthly invoices to City at the following address:

Special Terms and Conditions (if necessary)

The University has determined that Institutional Review Board or Institutional Animal Care and Use Committee review and approval are required in accordance with Article III of the Master Agreement, due to research on non-exempt human and/or vertebrate animal subjects:

Yes ☐ No ☐

Data Security Requirements

This project requires access to the following City data:

City Data is considered:

Personal Information	Yes ☐	No ☐
Highly Sensitive Personal Information	Yes ☐	No ☐
Austin Energy Confidential Information	Yes ☐	No ☐

Project Managers/Principal Investigator (PI)

UNIVERSITY

[Name of University Representative]
[Title of University Representative]
[Address]
Phone: 512-
Email:

CITY

[Name of City Representative]
[Title of City Representative]
[Address]
Phone: 512-
Email:

Project Manager(s) may be changed by mutual written agreement of the Parties.

Other Key Personnel Involved

The Effective Date of this Work Order is the date of last signature.

Executed by:

CITY OF AUSTIN	**UNIVERSITY**
Name: _____	Name: _____
Title: Director	Title: _____
Date: _____	Date: _____

Approved by City Project Manager:

By: _____
Name: _____
Title: _____
Date: _____

Approved as to Form:

By: _____
Name: _____
Title: Assistant City Attorney
Date: _____

Austin Energy Data Handling Controls	
Rev. No.: 2.0	Date: October 5, 2018
Owner: Enterprise Information Security	Category: Information Security
Author: Michael Goin	SME: Mike Goin, AE Risk Management, AE Legal
	Doc Type: Contract Exhibit

CONTENTS

1. DATA HANDLING CONTROLS: SECURITY DIRECTIVES AND REQUIREMENTS

1.1. Contractor Responsibilities regarding treatment of City Data

1.1.1. The City requires that controls ("Data Handling Controls" or "DHC") be in place to manage risk to the confidentiality, integrity and availability of City Confidential Information in any form in the care, custody or control of Contractor. These Data Handling Controls represent a minimum standard for protection. Additional controls required under applicable laws, regulations, or standards governing specific forms of data (e.g., health information, credit cardholder data) may also apply.

1.1.2. Contractor agrees to comply with these Data Handling Controls in performing the Services (including information technology-based Services) and in providing the Deliverables under the Contract. Contractor accepts all responsibility and liability for the security, integrity and protection of all City Data in its custody or control, including but not limited to when City Data is received, transmitted, processed, stored, backed up, archived, returned, or as occurs otherwise during performance of Services, including that involving a subcontractor. Contractor agrees that any damages or liability arising from any violation of these Data Handling Controls, including damage to City Data as well as all work to restore City Data and its integrity, are Contractor's responsibility. Contractor agrees that compliance with these Data Handling Controls is not an affirmative defense to any losses, disclosures, corruption or other damage to City Data which may occur for which Contractor is responsible, as Contactor acknowledges and agrees that there may be situations for which the Data Handling Controls may be inadequate to reasonably protect City Data as a project matures during the term of the Contract, and Contractor agrees to use appropriate additional measures in its reasonable judgment to protect City Data in such situations.

1.2. Location Parameters

1.2.1. The authorized geographical data center region for the storage and processing of City Data under this Contract is the contiguous United States.

1.2.2. Contractor may utilize non-US based personnel but must ensure that City Confidential Information cannot be stored, viewed, downloaded, or transported outside the contiguous United States.

1.3. Specific Security Directives

1.3.1. For access to City Data, Contractor must ensure that only the minimum amount of rights is granted to an Authorized Person as required to perform Contractor's contractual duties.

1.3.2. Unless otherwise approved by the City in advance, in writing, Contractor must encrypt all City Confidential Information. Only an Authorized Person within the Secure Service Area may view unencrypted City Confidential Information.

1.3.2.1. Contractor employees and subcontractors who have provided written certification showing they meet the minimum requirements of these Data Handling Controls are allowed to view unencrypted City Confidential Information if necessary to provide the Services.

1.3.2.2. The Secure Service Area shall be designed in such a way as to prohibit the unauthorized viewing, modification, or destruction of any unencrypted City Confidential Information (including any image). Contractor may not remove City Confidential Information from the Secure Service Area unless approved by the City in advance in writing.

1.3.3. Unencrypted City Confidential Information may not be stored on any Contractor or subcontractor Endpoint Device.

1.3.4. Contractor must have in place its own internal security program that includes policies using applicable industry best practices. Contractor will provide documentation of these policies and procedures within ten business days of written request by the City.

1.3.5. Contractor must detach all removable storage media containing City Confidential Information from any device when not in use and store the media in Contractor's physically-secure location.

1.3.6. Contractor must ensure that only an Authorized Person may access devices containing City Data.

1.4. Data Disposition

1.4.1. Contractor agrees to return all City Data obtained under this Contract (including this DHC) or otherwise in its care, custody or control to the originating City department, and to delete any remaining copies from Contractor's storage/production/use/possession at the end of the engagement, including:

1.4.1.1. as stated in any scope of work and/or

1.4.1.2. at City's request, or upon

1.4.1.3. Contractor's failure to follow the compliance directives of this Data Handling Controls document.

1.5. General Compliance Requirements

1.5.1 Contractor's failure to comply with any provision of these Data Handling Controls is a material default under the Contract.

1.5.2 Contractor agrees that City or its authorized representatives may audit or review Contractor's compliance with these Data Handling Controls under Contract Section 0300, Paragraph 17, Audits and Records. Except in an emergency (including a Breach or Security Incident), such audit or review shall be conducted only during normal business hours and without disrupting normal business practice, and City shall provide reasonable advance notice of exercising its right of audit or review.

Audits or reviews may include, but are not limited to:

- system, security, application, operating system, and database logs;
- physical access logs at all data centers;
- data center location or ownership changes;
- access control procedures;
- procedures for the physical and digital destruction of media;
- environment changes that have the potential for outages;
- workplace inspections for compliance with these Data Handling Controls and review of any Vendor supplied documentation submitted to document/demonstrate compliance; and
- procedures for and evidence of routine testing and updating of systems to prevent against attacks.

1.6. Logging/Auditing Requirements

1.6.1. Contractor must create system, security, application, operating system, and database logs:

1.6.1.1. when Contractor creates, reads, updates, or deletes City Data;

1.6.1.2. when Contractor initiates a network connection;

1.6.1.3. when Contractor accepts a network connection;

1.6.1.4. at user authentication and authorization, including failed access attempts;

1.6.1.5. for user login and logout;

1.6.1.6. when Contractor grants, modifies, or revokes access rights, privilege levels, and permissions, firewall rules, and user passwords;

1.6.1.7. when Contractor makes any system, network, or services configuration changes, including installation of software patches and updates, other installed software changes, operating system and Hypervisor activity;

1.6.1.8. at application process startup, shutdown, or restart;

1.6.1.9. in the case of any application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), and in cases of failure of network services, such as DHCP or DNS, or hardware fault; and

1.6.1.10. if contractor detects suspicious or malicious activity, such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

1.6.2. Contractor will retain system activity logs (and make all such logs available to City) for a period of three years after final payment on this Contract, or three years after all forensic, audit and litigation matters are resolved, whichever is longer.

1.6.3. Contractor will review all relevant security logs for anomalies for potential Security Incidents and forensic analysis.

1.7. Media Reuse

1.7.1. Contractor must promptly Securely Erase all City Confidential Information from any permanent or non-volatile storage media:

1.7.1.1. once immediate use of such media is no longer necessary,

1.7.1.2. at City's request, or

1.7.1.3. within 30 days of termination of the Contract.

1.7.2. For all endpoint and mobile devices containing City Data, Contractor agrees to utilize full disk encryption with pre-boot authentication methodologies to ensure all City Confidential Data is encrypted at rest.

1.7.3. Contractor shall Securely Erase all City Data by destructively overwriting all City Data to ensure that even deleted files cannot be recovered from the media.

1.8. Security

1.8.1. Contractor must limit access to the Hypervisor to only those qualified and pre-approved staff who have job functions dedicated to performing work on the Hypervisor. All access logs to the Hypervisor must only be reviewed by qualified personnel approved by Contractor and City.

1.8.2. City retains ownership over all City Data.

1.8.3. Contractor must use industry best practices for encryption of City Confidential Information at rest and in transit.

1.8.4. Contractor will ensure that all electronic and physical access to City Data is secured. Contractor must verify the identification, authentication, and authorization of each user and their specific role and access level, and Contractor must immediately block all physical and electronic access to City Data for any terminated employee.

1.8.5. Contractor must use due diligence to evaluate and respond to potential Security Incidents and events that create suspicions of unauthorized disclosure, modification, or destruction of City Data. The response must restore the confidentiality, integrity, and availability of the environment(s) compromised or potentially compromised, and establish root causes and remediation steps and determine the nature and extent of the event. If Contractor determines that there has been a Security Incident involving City Data (including City Confidential Information), Contractor shall report such Security Incident to the City PM within four (4) hours of determination.

1.8.6. Upon written request, Contractor shall make its then current key management policy for encryption keys and certificates available to the City within 10 business days.

2. DATA HANDLING CONTROLS: ADDITIONAL COMPLIANCE REQUIREMENTS

2.1. Contractor Practices

2.1.1. In addition to any other requirements of these Data Handling Controls, Contractor agrees it shall maintain and enforce its own reasonable and adequate security procedures during the term of the Contract for the protection of City Data, which procedures must be designed to protect City Data (especially City Confidential Information) and the hosting environment from a Security Incident, including using Contractor's best efforts to avoid the unauthorized access, modification or loss during transmission and storage, including the use of data encryption techniques described herein.

2.1.2. Contractor confirms that all use, transmission, storage, and destruction of City Confidential Information shall be in strict accordance with all terms, covenants, and conditions of the Contract and all applicable Federal, State, and local laws, rules, and regulations.

2.1.3. Contractor agrees that City may conduct, at no extra cost to City, network penetration tests of all systems at Contractor's facilities used for the processing,

storage or transmission of City Data. City may also, at its discretion, contract out penetration testing services to a third party. City shall provide reasonable notice of each network penetration test and shall conduct each network penetration test at reasonable times. If, following any testing, vulnerabilities are identified, Contractor shall promptly document Contractor's remediation action plan and provide it to the City PM within three business days, including at a minimum:

2.1.3.1.1. nature of the vulnerability including scope and breadth,

2.1.3.1.2. potential impact to service of vulnerability and subsequent mitigation,

2.1.3.1.3. summary of mitigation, and

2.1.3.1.4. known or suspected loss of City Data and ability to recover; and

2.1.3.2. implement the remediation action plan not later than three business days after delivery of the plan unless otherwise approved by City in writing. The implementation of remediation activity must be communicated to and approved by the City in advance, ensuring the avoidance of unplanned outages; and

2.1.3.3. provide City with written documentation and reports on the status of all modifications to correct such vulnerabilities, including interim and final reports.

2.1.4. Contractor shall perform appropriate background checks on its employees and subcontractors with access to City Confidential Information.

2.1.5. Contractor shall prohibit access to City Confidential Information for Contractor employees and subcontractors who fit into any of the following classifications:

2.1.5.1. Anyone who has been convicted of a felony offense;

2.1.5.2. Anyone who has been convicted of a misdemeanor offense related to computer security, theft, fraud or violence; or

2.1.5.3. Anyone who is currently awaiting trial for any of the above-stated offenses.

2.1.6. The COA CISO may, at any time in writing, require Contractor's employees and subcontractors to submit to additional background checks. Continued access to City Data, including City Confidential Information, and secured facilities shall be contingent on the Contractor's employee's agreement to submit to a background check and the results of the background check. Refusal shall be grounds for immediate termination of the User ID and password, and where applicable, access to COA premises and networks, and any ID badge issued shall immediately be decommissioned.

2.2. Security Incident Reporting Procedures

2.2.1. Contractor must telephone the City PM and e-mail AE-Exec-Info-Sec@austinenergy.com within four business hours of when Contractor discovers, is notified of, or otherwise has knowledge of any Security Incident. Contractor must include the following information in the report emailed:

2.2.1.1. person reporting the Security Incident ;

2.2.1.2. person who discovered the Security Incident;

2.2.1.3. date and time the Security Incident was discovered;

2.2.1.4. nature of the Security Incident;

2.2.1.5. actions taken and by whom;

2.2.1.6. involved system and possible interconnectivity with other systems;

2.2.1.7. description of the information lost or compromised, or potentially lost or compromised;

2.2.1.8. storage medium from which information was lost or compromised;

2.2.1.9. controls in place to prevent unauthorized use of the lost or compromised information;

2.2.1.10. number of individuals potentially affected;

2.2.1.11. whether law enforcement or other external agencies were involved for any reason and, if so, those contacted; and

2.2.1.12. any other relevant information pertaining to the Security Incident.

2.2.2. Within four hours of discovering the Security Incident, the Contractor shall contain the Security Incident.

2.2.3. Contractor shall investigate (with City's participation, if so desired by City) the Security Incident, perform a root cause analysis, and create and provide to the City a remediation plan within seven days of becoming aware of the Security Incident.

2.3. Remediation

2.3.1. As soon as practicable, and at no additional cost to the City, Contractor will remedy the source of the Security Incident, as required by the remediation plan.

2.3.2. The Contractor shall reimburse the City for all costs to City associated with the Security Incident.

2.4. Recovery

2.4.1. Within seven days of completing the remediation plan, Contractor must provide the City reasonable written assurance declaring full system recovery, signed by an executive with proper authority, attesting that the Security Incident is remediated and shall not recur.

2.5. Lessons Learned

2.5.1. Contractor shall, at no cost to the City and as part of the Services, update policies, procedures, or enforcement methods in a manner designed to prevent similar Security Incidents from recurring and provide summary of updates to City within 14 days of declaring full system recovery.

3. Definitions

3.1.1. **Authorized Person** – Contractor personnel (including subcontractor personnel) located in the contiguous United States having successfully completed the required background check and related requirements of the Contract

3.1.2. **City Project Manager or City PM** – City of Austin project manager, or their designee, assigned to this Contract

3.1.3. **City Data** - data or information (in any form) regarding the City or its customers that is created, collected, provided, obtained, or otherwise made available in connection with this Contract to an Authorized Person. City Data may be either non-confidential information or City Confidential Information.

3.1.4. **City Confidential Information** – includes: (A) information provided by City that is marked or identified as confidential, (B) information of City including software, computer programs, documentation, processes, procedures, techniques, technical, financial, customer, personnel and other business information of a non-public nature that would reasonably be understood to be confidential whether or not marked or identified as confidential, (C) information generated by Contractor (or subcontractor) that contains, reflects, or is derived from confidential information, (D) Personal Identifying Information, (E) Sensitive Personal Information, and (F) all other information made confidential by federal, state or local law or regulation. City Confidential Information is a subset of City Data.

3.1.5. **Data Center Region** – means the authorized geographical region for the storage and processing of City Data, and is presently only the contiguous United States.

3.1.6. **Data Handling Controls** – this document

3.1.7. **Endpoint Device** – Any network-capable computer hardware device including, but not limited to desktop computers, laptops, smart phones, tablets, thin

clients, printers or other specialized hardware such POS terminals and smart meters.

3.1.8. **Hypervisor** – a piece of computer software, firmware or hardware that controls the flow of instructions between guest Operating Systems and the physical hardware such as CPU, disk storage, memory, and network interface cards within a virtual environment

3.1.9. **Personal Identifying Information** ("PII") – means any information that, either alone or in conjunction with other information, identifies an individual, including an individual's:

3.1.9.1. name, social security number, date of birth, or government-issued identification number;

3.1.9.2. mother's maiden name;

3.1.9.3. unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; or

3.1.9.4. unique electronic identification number, address, or routing code

3.1.10. **Sensitive Personal Information** ("SPI") – means

A. an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(i) Social Security Number;

(ii) Driver's License Number or government-issued ID; or

(iii) an individual's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account, or

B. information that identifies an individual and relates to the physical or mental health or condition of the individual, or the provision of health care to the individual.

C. SPI does not include publicly available information.

3.1.11. **Securely Erase** – secure deletion of any information, including a recognized destructive delete algorithm, for example, at least seven overwrites with pseudorandom data or at least seven overwrites with zeroes

3.1.12. **Security Incident** – any actual or potential unauthorized disclosure of, or unauthorized access to, City Confidential Information; or a violation or imminent threat of violation of computer security policies, acceptable use policies, or compliance requirements under these Data Handling Controls; or violation or imminent threat of violation of industry standard security practices

3.1.13. **Secure Service Area** – a physically and electronically secured area, with secure communications, within Contractor's facility where unencrypted City Confidential Information is secured from unauthorized access

