INTERLOCAL DATA-SHARING AGREEMENT

This Interlocal Data Sharing Agreement (this "Agreement") is entered into by and between the City of San Antonio, Bexar County Appraisal District, CPS Energy, San Antonio Housing Authority, San Antonio River Authority, San Antonio Water System, and VIA Metropolitan Transit, individually referred to herein as "Entity" or "Party" and collectively referred to herein as "Entities" or "Parties".

RECITALS

WHEREAS, the Greater San Antonio Metropolitan Area encompasses multiple municipal governments, other local governments, and state agencies, all of which rely on data to perform and improve their respective services, manage internal operations, and interact with the public; and

WHEREAS, the Parties agree that ensuring the privacy and safekeeping of Confidential Information in their possession is of the highest priority; and

WHEREAS, the responsible integration of certain data possessed by the various Entities would enable Smart City solutions that facilitate the improvement in the delivery of programs and services by all of the Entities to the citizens of San Antonio; and

WHEREAS, the Parties wish to work cooperatively to achieve the following goals:

- Establishing a sustainable framework for facilitating mutually-beneficial cooperation between and among Entities for the purpose of better serving the members of the public who access their respective program and service offerings;

- Developing and implementing data-driven policies and programs that best align with local needs;

- Demonstrating the feasibility and value of the shared and integrated data;

- Ensuring the protection of privacy and Confidential Information through data security measures and clear processes for handling and storing shared data;

- Establishing standards for the exchange of Confidential Information in a usable format; and

WHEREAS, this Agreement supports the Smart City initiative, which will enable the Parties to share data in an appropriate and mutually agreeable manner so as to make more informed decisions for the benefit of their constituents; and

WHEREAS, the Parties wish to outline conditions under which the Entities will share and use data and the procedures to be adopted by each participating Entity to ensure

the proper transfer, handling, storage, and protection of data for the benefit of the public; and

WHEREAS, Chapter 791 of the Texas Government Code allows local governments and state agencies to enter into interlocal cooperation agreements for their mutual benefit and performance of governmental and administrative functions that each Entity is authorized to perform independently; and

WHEREAS, Chapter 552 of the Texas Government Code, known as the Public Information Act (the "Act"), specifically allows for the transfer of data exempt from public disclosure between Governmental Bodies as defined by the Act, and in interpreting the Act, the Texas Attorney General has opined that the transfer of such data in this manner does not constitute a release of the data to the public for purposes of the Act and does not violate the confidentiality of the data or waive the exceptions to public disclosure that the transferring Governmental Body may have under the Act; and

WHEREAS, the Parties wish to enter into this Agreement to facilitate the responsible and secure exchange of Data for the benefit and betterment of the citizens of San Antonio, Texas; and

THEREFORE, the Parties, acting by and through their respective Governing Bodies, individually and collectively, do hereby adopt the conditions set forth in this Agreement and mutually agree as follows:

ARTICLE I
DEFINITIONS

Definitions. The following terms used in this Agreement have the meanings set forth below, unless otherwise stated.

1.1. "Authorized User" means an employee or agent of a Receiving Entity who has (i) executed the authorization form attached as Attachment D – Confidentiality Agreement for Authorized User, and (ii) been authorized by such Receiving Entity to access Data in order to fulfill the official duties of such employee or agent.

1.2. "Breach" means the unauthorized acquisition, access, or disclosure of physical or electronic Confidential Information belonging to another Party that compromises the security, confidentiality, or integrity of such Confidential Information.

1.3. "Confidential Information" means Data in the possession of a Party (the "Disclosing Entity") which falls into or under any exception contained in the Act. Confidential Information shall not include any Data that has been voluntarily disclosed to the public by the Disclosing Entity (except where such public disclosure has been made by the Receiving Entity without authorization) or that has been independently developed and disclosed by others, or that otherwise enters the public domain through lawful means without breach of any obligations

2

of confidentiality owed to the Disclosing Entity.

1.4. "Data" means any Public or Confidential Information that has been shared by a Disclosing Entity with a Receiving Entity pursuant to this Agreement.

1.5. "Data Owner" means the Entity which owns or controls access to Data and who maintains and manages such Data.

1.6. "Data Request Form" means the form attached hereto at Attachment A.

1.7. "Data Sharing" is the act of a Disclosing Entity sharing Data with a Receiving Entity pursuant to this Agreement.

1.8. "Data Sharing Consortium" refers collectively to the names of the Entities participating in this Agreement.

1.9. "Disclosing Entity" means the Data Owner who releases the Data under the terms of Attachment A – Data Request Form.

1.10. "Information Coordinator" means the single point of contact appointed by each Entity to make and receive Data requests on behalf of that Entity, and the responsible Entity representative to search, find, and share requested Data subject to the conditions, if any, set forth in a Data Request Form that has been executed by the relevant Disclosing Entity and Receiving Entity.

1.11. "Governmental Body" has the same meaning as the term is defined in Section 552.003(1)(A) of the Texas Government Code.

1.12. "Public Information" has the same meaning as that term is defined in Section 552.002(a) of the Texas Government Code and shall not be considered Confidential Information.

1.13. "Receiving Entity" means the Entity who receives Data from a Disclosing Entity pursuant to a Data Request Form that has been executed by such Entity and Disclosing Entity.

1.14. "State Agency" has the same meaning as the term "Agency" as defined in Section 771.002(1) of the Texas Government Code.

1.15. "Technical Working Group" means the working group described in Section 2.5.2.

ARTICLE II
DATA SHARING FRAMEWORK

2.1. Framework. This Agreement establishes the rules and procedures for engaging in Data Sharing for the purposes set forth in, and in accordance with the requirements established by, this Agreement. For purposes of clarity, the prerequisites for engaging in Data Sharing shall include the completion of

SmartSA Executive Committee policies necessary and appropriate for Data Sharing as further discussed in Section 2.5.1 below, completion of the Data Sharing training program as further discussed in Section 2.4 below, and the completion of the technical standards and security protocols for the exchange of Data and protection of Confidential Information as further discussed in Section 2.5.2 below. Once the prerequisites have been met, any Entity may request Data from another Entity pursuant to this Agreement by completing the Data Request Form in Attachment A and submitting it to the other Entity.

2.2.   Roles. Each participating Entity shall be considered a Disclosing Entity with respect to Data it shares with a Receiving Entity, and a Receiving Entity with respect to Data it receives from a Disclosing Entity.

2.3.   Expenses. No Party shall be required to provide any financial reimbursement to any other Party for executing this Agreement or engaging in Data Sharing pursuant to this Agreement; *provided, however,* that any Parties may voluntarily agree to any financial reimbursement arrangement with respect to any Data Sharing so long as such financial reimbursement arrangement is explicitly set forth in the executed Data Request Form pursuant to which the relevant Data is shared; *provided, further, however*, that nothing in this Agreement shall be interpreted as prohibiting any Party from entering into other agreements to facilitating the sharing of any type of Data or the reimbursement of expenses associated with such sharing.

2.4.   Training. The Parties shall cooperate to establish a Data Sharing training program. The details of the training program shall be specified and agreed upon by the Parties after execution of this Agreement by the Parties; provided, however, that any Party that subsequently executes this Agreement can request that all Parties cooperate to amend the Data Sharing training program to reflect the needs or wishes of all current Parties to the Agreement. Training materials may be made available to any Authorized User at any time after this Agreement is executed, but each Authorized User must have access to the training materials, and have completed the then current version of the Data Sharing training program before such Authorized User may have access to Confidential Information received from a Disclosing Entity pursuant to this Agreement.

2.5.   Governance. The Parties hereby (i) adopt the SmartSA governance structure set forth in Attachment E, and (ii) appoint the SmartSA Executive Committee as the leadership body to provide guidance to the Data Sharing Consortium.

2.5.1.   SmartSA Executive Committee. The SmartSA Executive Committee shall establish policies necessary and appropriate for Data Sharing by the Parties pursuant to this Agreement after execution of this Agreement by the Parties, which the SmartSA Executive Committee may amend from time to time. The SmartSA Executive Committee may create working groups to address specific technical or policy issues as necessary. The SmartSA Executive Committee shall consider recommendations from the

Technical Working Group and adopt generally applicable technical standards and security protocols for use by the Data Sharing Consortium. Each Entity shall designate a primary representative to participate in the Committee as well as a backup delegate for when the primary is unable to attend. Decisions by the SmartSA Executive Committee shall be made via majority vote, and each committee member shall only be allowed one (1) vote. The Parties shall comply with policies adopted by the SmartSA Executive Committee; *provided, however*, that in the event of a conflict between any policy adopted by the SmartSA Executive Committee and this Agreement, this Agreement shall prevail.

2.5.2. <u>Technical Working Group</u>. The Technical Working Group shall develop initial technical standards and security protocols for the exchange of Data and protection of Confidential Information after execution of this Agreement by the Parties. The Technical Working Group shall review, as necessary but no less than once a year, the existing technical standards and security protocols and make recommendations to the SmartSA Executive Committee regarding the adoption of any hardware or software upgrades or enhanced security protocols. Each Entity shall designate a primary representative to participate in the Working Group as well as a backup delegate for when the primary is unable to attend. Decisions by the Technical Working Group shall be made via majority vote, and each group member shall only be allowed one (1) vote. The Parties shall comply with any technical standards and security protocols adopted by the Technical Working Group and explicitly approved by the SmartSA Executive Committee; *provided, however*, that in the event of a conflict between any technical standards and security protocols approved by the SmartSA Executive Committee and this Agreement, this Agreement shall prevail.

2.6. <u>Meetings</u>. The SmartSA Executive Committee shall call a meeting of the Data Sharing Consortium no less than once each calendar year to discuss any relevant issues arising from this Agreement. The SmartSA Executive Committee shall define the agenda for the meetings and provide reasonable advance notice to the Parties prior to the meetings. Any two or more Parties may hold additional meetings at any time at their discretion to discuss any issue.

2.7. <u>Branding</u>. The City of San Antonio hereby grants a non-exclusive, non-transferable, non-sublicensable, limited duration license to each other Party to use the SmartSA mark on or in connection with the advertising and promotion of the SmartSA initiative in conjunction with the Party's efforts that utilize shared data under this Agreement so as to advance public awareness and appreciation of the collaboration. The City of San Antonio hereby reserves the rights not expressly granted to the Parties under this Section 2.7, and, without limiting the foregoing, all rights granted to the Parties under this Section 2.7 are subject to the City of San Antonio's reserved right to use the mark in its respective business, including in connection with the advertising and promotion of the SmartSA initiative in conjunction with the Parties' efforts. The Parties hereby acknowledge and agree

that any goodwill arising from any Party's use of the mark exclusively inures to the benefit of and belongs to the City of San Antonio. Upon the suspension or termination of this Agreement with respect to any particular Entity, other than the City of San Antonio, the suspended or terminated Entity's right to use the SmartSA mark shall automatically cease. Upon the suspension or termination of this Agreement with respect to the City of San Antonio, all other Entity's right to use the SmartSA mark shall automatically cease.

ARTICLE III
TERM

3.1.   This Agreement becomes effective upon the date it is signed by the last Party (the "Effective Date"), and shall continue in full force and effect through December 31st of the same calendar year as the Effective Date (the "Initial Term"), and will automatically renew for successive additional periods of one (1) year, unless or until terminated by all participating Entities pursuant to this Agreement by each Entity providing written notice of termination to all other Entities; provided, however, that, following termination of this Agreement, each Party shall remain subject to the requirements of this Agreement with respect to any Data it has received from any Disclosing Party until such time as the relevant Data is destroyed pursuant to the requirements of this Agreement or returned to the relevant Disclosing Party.

ARTICLE IV
SUSPENSION AND TERMINATION

4.1.   Any Entity may terminate its participation in this Agreement at any time by providing all other Entities thirty (30) days prior written notice of such termination; provided, however, that such Party shall remain bound by this Agreement with respect to any Data it has received from any Disclosing Party until such time as the Data is destroyed pursuant to the requirements of this Agreement or returned to the relevant Disclosing Party.

4.2.   If an Entity materially violates any requirement of this Agreement, the SmartSA Executive Committee may suspend or terminate the Agreement with respect to that particular Entity and require the Entity to return or destroy any Data it had previously received from a Disclosing Entity pursuant to this Agreement by providing the Entity with written notice of suspension or termination with an explanation of the basis for the suspension or termination.

4.3.   If a Receiving Entity materially violates any requirement of this Agreement with respect to any Data it received from a Disclosing Entity, the Disclosing Entity may, by providing written notice with explanation to such Disclosing Entity: (i) require the Receiving Entity to return or destroy an Data it previously shared with the Receiving Entity; and/or (ii) refuse to share any additional Data with the Receiving Entity.

4.4.   Any suspension or termination under this Article IV shall become effective immediately upon provision of written notice of such suspension or termination to the Information Coordinator for the suspended or terminated Entity; *provided, however*, that the Parties shall cooperate in good faith to resolve any dispute about whether the basis for a suspension or termination is valid.

4.5.   Any Entity alleged to have violated this Agreement shall cooperate in good faith in the investigations of the alleged violation.

ARTICLE V
RECEIVING ENTITY OBLIGATIONS

5.1.   Data Request Form Submissions. Any Entity may submit, through its Information Coordinator, a signed Data Request Form to the Information Coordinator of any other Entity at any time pursuant to this Agreement. By submitting a signed Data Request Form to another Entity, the submitting Entity represents and warrants that:

    5.1.1.   the Data it has provided in the Data Request Form is complete and accurate;

    5.1.2.   it has the legal authority to possess and use the requested Data as specified in the Data Request Form; and, with respect to the Data requested in the Data Request Form; and

    5.1.3.   the Entity submitting the Data Request Form will comply with:

        5.1.3.1.   the requirements of this Agreement;

        5.1.3.2.   any use limitations, data security requirements, confidentiality requirements, and any other restrictions specified in the Data Request Form; and

        5.1.3.3.   the Act.

5.2.   Confidentiality. A Receiving Entity shall not, either directly or indirectly, make any unauthorized disclosure of Confidential Information received via Data Sharing, and shall take reasonable measures to prevent unauthorized disclosures. Other than for the purpose of developing SmartSA projects and insights approved by Executive Committee, the Receiving Entity shall not distribute, reprint, alter, sell, assign, edit, modify, or create derivative works or any ancillary materials from or with the Confidential Information without prior written consent obtained in accordance with this Agreement. The Receiving Entity shall limit access to Confidential Information only to Authorized Users and Information Coordinators identified in Attachment B that have executed a Confidentiality Agreement Form as provided in Attachment D.

5.3.   Changes to Security Standards. A Receiving Entity shall provide prior written notice to all relevant Disclosing Entities with respect to any proposed changes to policies and procedures that deviate from explicit requirements that apply to Shared Data or that may materially increase the risk of unauthorized disclosure of any Confidential Information; *provided, however*, that the Receiving Entity shall, at the option of the Disclosing Entity, destroy or return all Confidential Information affected by any proposed change unless the Receiving Entity abandons the proposed change or negotiates a compromise that is acceptable to the Disclosing Entity.

5.4.   Internal Procedures. The Receiving Entity shall ensure that adequate internal controls, safeguards, and/or countermeasures are established to protect Confidential Information. All preventative, detective, and/or corrective controls shall be risk based. The Receiving Entity agrees to protect Confidential Information against unauthorized access or disclosure and to comply with the following measures:

5.4.1.   Confidential Information in physical or electronic format shall be stored and processed in such a way that unauthorized persons cannot access or retrieve the Confidential Information by any means, including, but not limited to, by computer or remote terminal.

5.4.2.   The Receiving Entity shall, as soon as possible, report to the Disclosing Entity all confirmed Breaches of any Confidential Information provided by the Disclosing Entity pursuant to an executed Data Request Form.

5.4.3.   Regarding a Breach that threatens or results in the disclosure of any Confidential Information, the Technical Working Group shall develop a protocol for investigating and confirming whether such a Breach has occurred. The Disclosing Entity shall be notified by the Receiving Entity within 24 hours of initiating the investigation protocol. Upon confirmation of a Breach, and following notification to the Receiving Entity's management team, the Receiving Entity shall notify the Disclosing Entity of the Breach and explain the nature of the Breach. Such notification must be provided within 72 hours after confirming the Breach. Should the Receiving Entity conclude that no Breach occurred, it shall notify the Disclosing Entity that it has concluded the investigation protocol and no Breach was detected.

5.4.4.   The Receiving Entity must, at all times, be able to confirm ability to properly accept, protect, and retain Confidential Information.

5.4.5.   The Receiving Entity agrees to make all Authorized Users that will have access to Data under this Agreement aware of the requirements of this Agreement, the Disclosing Entity's confidentiality and disclosure requirements, and the consequences of violating those confidentiality and disclosure requirements. Only Authorized Users who are listed on the

Data Request Form shall be given access to Confidential Information, including online files. All Authorized Users granted access to the Confidential Information, covered by this Agreement, shall be required to sign a Confidentiality Agreement Form, in the format provided in Attachment D, prior to being allowed access to the Confidential Information. The Receiving Entity shall obtain and store the original executed Confidentiality Agreement Forms as well as provide a copy to the Disclosing Entity. The Authorized Users shall be identified on the Data Request Form. Authorized Users with online access to Confidential Information shall access such information using only their personally assigned user IDs, which shall not be shared. The Receiving Entity shall guarantee within seven (7) business days of separation that Authorized Users who leave employment no longer have access to the Data. The Receiving Entity shall recertify any Authorized User who changes roles within the organization that still has a need to access the Data as originally documented on the Data Request Form. Upon request, the Receiving Entity must ensure that Data is subject to access by authorized personnel for review in a controlled environment.

5.5.   Inspection of Records. The Receiving Entity shall maintain and, upon request by the Disclosing Entity, provide to the relevant Disclosing Entity written records of:

  5.5.1.   all Data received pursuant to this Agreement, including a description of the Data, the authorized Information Coordinator who received the Data, and the date of receipt of such Data;

  5.5.2.   the location of storage for all received Data (*e.g.,* file path);

  5.5.3.   methods used to protect Confidential Information from access by unauthorized users (*e.g*., hidden or encrypted);

  5.5.4.   methods used to transmit Confidential Information, both internally and externally;

  5.5.5.   the names of all Authorized Users who have access to Confidential Information; and

  5.5.6.   the details regarding all confirmed Breaches of Confidential Information (*i.e*., unauthorized access to Confidential Information), including affected Confidential Information, the nature of the confirmed Breach, actions taken to ensure that similar Breaches do not occur in the future, notifications made to the Disclosing Entity, and remedial efforts taken.

A Disclosing Entity may not request written records more than once per calendar year. Notwithstanding the foregoing, a Disclosing Entity may request written records at any time the Disclosing Entity reasonably believes that the Receiving Entity is in breach of this Agreement, even if such Disclosing Entity has already requested written records pursuant to this Agreement one or more times during

the same calendar year.

5.6. <u>Data Destruction</u>. Each Receiving Entity is responsible for determining whether the destruction expectations of the Disclosing Entity are consistent with the Receiving Entity's own document control schedule and retention requirements, and to reconcile such inconsistencies with the Disclosing Entity prior to finalizing any Data Request Form.

5.7. <u>Third Party Data Requests</u>. If a Receiving Entity receives a request for Confidential Information by a third party, the Receiving Entity shall notify the appropriate Disclosing Entity within two (2) business days of receiving the request, and the Receiving Entity shall fully cooperate with the Disclosing Entity in opposing any such request to the extent permitted by applicable law.

ARTICLE VI
<u>DISCLOSING ENTITY RIGHTS AND OBLIGATIONS</u>

6.1. <u>Returned Data Request Forms</u>. By returning a signed Data Request Form to another Entity, an Entity represents and warrants that:

6.1.1. it has the legal authority to share the requested Data specified in the Data Request Form in accordance with the requirements of the Agreement and any additional restrictions or requirements set forth in the Data Request Form;

6.1.2. it has specified in the Data Request Form any and all additional requirements (*e.g*., encryption, use limitations) necessary to ensure that the requested Data can be shared and used as described in the Data Request Form pursuant to the Agreement and any additional restrictions and requirements specified in the Data Request Form in full compliance with applicable law; and, with respect to the Data requested in the Data Request Form; and

6.1.3. it approves and will comply with:

6.1.3.1. the requirements of this Agreement;

6.1.3.2. any other restrictions set forth in the Data Request Form; and

6.1.3.3. the Act.

6.2. <u>Denials</u>. An Entity may deny, in full or in part, a Data Request Form received from the Information Coordinator of another Entity when:

6.2.1. it does not have the legal authority to share the requested Data for the proposed uses specified in the Data Request Form;

6.2.2. it reasonably believes that sharing the requested Data for the proposed

uses specified in the Data Request Form may cause reputational or operational harm to one or more Parties;

6.2.3. it reasonably believes that the requested Data cannot be adequately protected or secured when shared or used in the manner specified in the Data Request Form;

6.2.4. it does not possess the Data requested; and/or

6.2.5. the Data Request Form failed to identify the correct Information Coordinator.

6.3. No Transfer. No patent, copyright, trademark or other proprietary right is licensed, granted or otherwise transferred to a Receiving Entity by the act of Data Sharing under this Agreement. The Disclosing Entity reserves all rights to Data in its possession and as distributed to any Requesting Entity.

6.4. **DISCLAIMER. THE DATA PROVIDED BY A DISCLOSING ENTITY TO THE RECEIVING ENTITY IS PROVIDED "AS IS" AND WITHOUT ANY WARRANTIES OF ANY TYPE, EXPRESS OR IMPLIED, BY THE DISCLOSING ENTITY. THE DISCLOSING ENTITY DOES NOT WARRANT, REPRESENT, OR GUARANTEE THAT THE DATA IS CORRECT, ACCURATE, OR FIT FOR ANY PARTICULAR PURPOSE AS OF THE DATE THE DATA IS PROVIDED TO THE RECEIVING ENTITY. THE DISCLOSING ENTITY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY, ANY IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY OF NONINFRINGEMENT, AND ANY EXPRESS WARRANTY WITH RESPECT TO ANY OF THE DATA AND DOCUMENTATION DISCLOSED HEREUNDER. THE DISCLOSING ENTITY ACCEPTS NO RESPONSIBILITY AS A RESULT OF ANY EXPENSES, LOSSES, DAMAGES, OR ACTIONS INCURRED OR UNDERTAKEN BY THE RECEIVING ENTITY AS A RESULT OF THE RECEIPT, MANIPULATION, OR USE OF ANY DATA OR DOCUMENTATION.**

ARTICLE VII
ROLE OF INFORMATION COORDINATORS

7.1. Data Request Process. Upon receiving a signed Data Request Form, an Information Coordinator shall promptly review and provide the Information Coordinator who submitted the Data Request Form with:

7.1.1. an approval of the request by returning a signed Data Request Form, which will become effective when the Receiving and Disclosing Entity both sign the Data Request Form; or

7.1.2. a full or partial denial with the reasons for such denial, in which case the other Information Coordinator may, but is not required to, submit a new Data Request Form in order to eliminate the reasons for such full or partial denial, which the receiving Information Coordinator will process in accordance with this request process.

Upon receipt and review of a Data Request Form, the Information Coordinator of an Entity will inform the Information Coordinator who submitted the Data Request Form as soon as possible if more than thirty (30) days will be necessary to respond to the Data Request Form along with an estimated response date.

7.2. Information Coordinators.

7.2.1. All requests for Data shall be coordinated through the respective Information Coordinators listed in Attachment B for the relevant Entities.

7.2.2. Any Entity may change its designated Information Coordinator at any time by providing the other Entities with written notice of the change.

7.2.3. The Information Coordinator for each Disclosing Entity is responsible for internally vetting any request for Data made by an Entity submitting a Data Request Form in accordance with this Agreement and the Disclosing Entity's internal processes, standards, and procedures.

7.2.4. The Disclosing Entity's Information Coordinator shall identify the Data that is acceptable for Data Sharing and identify any and all additional requirements that the Disclosing Entity deems reasonable and necessary to impose on the Receiving Party based on the requested Data.

7.2.5. The Information Coordinator shall use reasonable efforts to respond in a timely manner to each Data request, ensure that the Data Request Form is complete and accurate, and process, publish, and transfer the Data as mutually agreed upon in the Data Request Form.

ARTICLE VIII
SECURITY AND PROTECTION OF CONFIDENTIAL INFORMATION

8.1. Transfer. Data Sharing pursuant to this Agreement shall only be undertaken in strict accordance with the requirements of this Agreement, the relevant Data Request Form, and any protocols, policies, technical and security requirements developed by the Technical Working Group, Executive Committee, and any other committee or subject matter expert established by the Executive Committee. The Disclosing Entity shall ensure that Confidential Information is encrypted when digitally transferred or is placed in a tamper-proof container/packaging when physically transferred to the Receiving Entity. The acceptable level of security and encryption for transfers shall be determined by the Technical Working Group, unless the Disclosing and Receiving Entity describe otherwise in the Data Request Form. The Receiving Entity shall coordinate any internal infrastructure

modifications that must be made to receive the Data as directed, prior to its receipt.

8.2. <u>Storage</u>. If the Data requested is Confidential Information, as determined by the Disclosing Entity, the Receiving Entity agrees to store the Confidential Information received under this Agreement in a secure manner. The acceptable level of security and encryption for storage shall be determined by the Technical Working Group, unless the Disclosing and Receiving Entity describe otherwise in the Data Request Form. For online access to Confidential Information, the Receiving Entity agrees to implement reasonable internal controls to comply with this Agreement and to prevent unauthorized access to the information system or database storing the Confidential Information. The Receiving Entity agrees to permit authorized personnel of the Disclosing Entity to make reasonable access for on-site review and inspection of the Receiving Entity's security measures as necessary to review the Confidential Information required under Section 5.5 (Inspection of Records). The Parties agree to comply with all applicable state and federal laws, regulations, and the security requirements described herein. Confidential Information shared pursuant to this Agreement shall only be stored on a device owned, issued, or approved by the Receiving Entity, subject to internal controls of the Receiving Entity. Each party must ensure that Confidential Information that is stored, processed, and/or transmitted using a personal device is protected pursuant to internal controls. The Receiving Entity shall not maintain in storage any Confidential Information longer than is absolutely necessary.

8.3. <u>Authorization</u>. The Disclosing Entity shall be deemed to have obtained all necessary internal organizational authorization and other required prerequisites to ensure the Disclosing Entity may represent itself as the Disclosing Entity prior to sharing the Data with the Requesting Entity. The Receiving Entity may rely on the representation made by the Disclosing Entity that such approvals have been obtained. Failure by the Disclosing Entity to obtain such approval prior to Data Sharing may result in a termination of participation in this Agreement as decided by the SmartSA Executive Committee.

ARTICLE IX
TEXAS PUBLIC INFORMATION ACT EXCEPTION

9.1. The Parties acknowledge that Confidential Information received from a Disclosing Entity is excepted from required disclosure under the Texas Public Information Act, Texas Government Code, Chapter 552. It is the Parties' understanding and opinion, as confirmed by each Party's legal counsel that the Texas Attorney General has recognized that Governmental Bodies, such as the Parties, may share Confidential Information in the manner contemplated by this Agreement. The sharing of Confidential Information, as provided herein, does not constitute a public disclosure of Confidential Information or a waiver of any exception to public disclosure under the Texas Public Information Act.

ARTICLE X
ASSIGNMENT /TRANSFER OF INTEREST/CONFIDENTIALITY

10.1. No Party may assign or transfer its rights, privileges, or obligations under this Agreement without prior written approval by all other participating Entities. Any attempt to assign or transfer without such approval is void.

ARTICLE XI
LEGAL CONSTRUCTION

11.1. Choice of Law. This Agreement is governed by the laws, codes, and regulations of the U.S. and the State of Texas, all of which are subject to change. This Agreement shall be construed under and in accordance with the laws of the State of Texas, and all obligations of the Parties created hereunder are performable in Bexar County, Texas. Venue shall be exclusively in the Federal or State Courts located in Bexar County, Texas.

11.2. Change of Law. Upon applicable state law or regulation change, this Agreement shall be considered immediately modified in accordance with each such change, without notice or written amendment. This provision for automatic amendment shall not apply where one Party provides written notice to the other Parties and SmartSA Executive Committee within sixty (60) days after the effective date of the state law or regulation change that it desires to amend the Agreement. Upon giving the required notice, the Parties agree to negotiate the effect the particular federal or state law or regulation change will have on this Agreement.

11.3. Compensation. Except as otherwise stated in this Agreement, no Party is required to pay compensation to another Party or that Party's personnel for services rendered hereunder.

11.4. Severability of Contractual Provisions. In the event one or more of the provisions contained in this Agreement shall, for any reason, be held to be invalid, illegal, or unenforceable in any respect, such invalid, illegal, or unenforceable provision shall not affect any other provision hereof, and this Agreement shall be construed as if such invalid, illegal, or unenforceable provision had never been contained herein.

11.5. No Waiver of Rights. Unless otherwise specifically provided for in this Agreement, a waiver by any Party of a breach of any of the terms, conditions, covenants or guarantees of this Agreement shall not be construed or held to be a waiver of any succeeding or preceding breach of the same or any other term, condition, covenant or guarantee herein contained. Further, any failure of any Party to insist in any one or more cases upon the strict performance of any of the covenants of this Agreement, or to exercise any option herein contained, shall in no event be construed as a waiver or relinquishment for the future of such covenant or option. In fact, no waiver, change, modification, or discharge by any Party hereto of any provision of this Agreement shall be deemed to have been

made or shall be effective unless expressed in writing and signed by the Party to be charged. No act or omission by a Party shall in any manner impair or prejudice any right, power, privilege, or remedy available to that Party hereunder or by law or in equity, such rights, powers, privileges, or remedies to be always specifically preserved hereby.

11.6. Injunctive Relief. The Parties agree that an impending or existing violation of any provision of this Agreement by a Party which would cause the Disclosing Entity irreparable injury for which it would have no adequate remedy at law, the Disclosing Entity shall be entitled to obtain immediate injunctive relief prohibiting such violation, in addition to any other rights and remedies available.

11.7. Attorney's Fees. In the event of litigation, each Party is responsible for its attorney's fees.

11.8. IN NO EVENT SHALL A PARTY BE LIABLE TO ANOTHER PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, REGARDLESS OF THE CAUSE OF ACTION, ARISING OUT OF OR IN CONNECTION WITH A PARTY'S PERFORMANCE.

ARTICLE XII
AMENDMENTS

12.1. No amendment, modification, or alteration of the terms hereof shall be binding unless the same is in writing, dated subsequent to the date hereof and duly executed by the Parties hereto, and authorized by each Party's governing body, as may be required.

ARTICLE XIII
NOTICES

13.1. All notices provided to be given under this Agreement shall be sent to the persons and addresses designated in Attachment C. Notices shall be in writing and shall either be personally served against a written receipt therefore or given by certified mail or registered mail, return receipt requested, postage prepaid, and addressed to the proper Party at the address specified in Attachment C, as may be updated from time to time. All notices given by mail shall be deemed to have been given at the time of deposit in the United States mail and shall be effective from such date.

ARTICLE XIV
FORCE MAJEURE

14.1. No Party shall be responsible for delays or lack of performance, which result from acts beyond a Party's reasonable control or caused by Acts of God, strikes or other labor disturbances, or delays by federal or state officials in issuing necessary regulatory approvals and/or licenses. In the event of any delay or failure excused by this Article XIV, the time of delivery or of performance shall be extended for a reasonable time period to compensate for said delay.

ARTICLE XV
INCORPORATION OF ATTACHMENTS

15.1.   Each of the Attachments listed below is an essential part of this Agreement, all of which are attached hereto and are incorporated into this Agreement by this reference, with this Agreement taking priority over all Attachments:

Attachment A – Data Request Form

Attachment B – Information Coordinators

Attachment C – Persons and Addresses for Notice

Attachment D – Confidentiality Agreement Form

Attachment E – SmartSA Governance Structure

ARTICLE XVI
PARTIES BOUND

16.1.   This Agreement shall be binding on and inure to the benefit of the Parties hereto and their respective heirs, executors, administrators, legal representatives, and successors and assigns, except as otherwise expressly provided for herein.

ARTICLE XVII
ENTIRE AGREEMENT

17.1.   This Agreement, together with its authorizing ordinance and its exhibits, if any, constitute the final and entire agreement between the Parties hereto and contain all of the terms and conditions agreed upon. No other agreements, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or to bind the parties hereto, unless they are in writing, dated subsequent to the date hereto, and duly executed by the Parties.

IN WITNESS WHEREOF, the undersigned certifies by execution of this Agreement that the undersigned is the duly authorized representative of the signatory Party with the requisite authority to execute this Agreement on the Party's behalf.

Signatures for execution on the following pages.

EXECUTED and **AGREED** to as of the dates indicated below.

CITY OF SAN ANTONIO

_____

(Signature)

Printed Name: _____

Title: _____

Date: _____

Approved as to Form:

_____

Assistant City Attorney

EXECUTED and **AGREED** to as of the dates indicated below.

BEXAR COUNTY APPRAISAL DISTRICT

_____

(Signature)

Printed Name: _____

Title: _____

Date: _____

EXECUTED and **AGREED** to as of the dates indicated below.

CPS ENERGY

_____

(Signature)

Printed Name: _____

Title: _____

Date: _____

EXECUTED and **AGREED** to as of the dates indicated below.

SAN ANTONIO HOUSING AUTHORITY

_____
(Signature)

Printed Name: _____
Title: _____
Date: _____

EXECUTED and **AGREED** to as of the dates indicated below.

SAN ANTONIO RIVER AUTHORITY

_____
(Signature)

Printed Name: _____
Title: _____
Date: _____

EXECUTED and **AGREED** to as of the dates indicated below.

SAN ANTONIO WATER SYSTEM

_____

(Signature)

Printed Name: _____
Title: _____
Date: _____

EXECUTED and **AGREED** to as of the dates indicated below.

VIA METROPOLITAN TRANSIT

_____
(Signature)

Printed Name: _____

Title: _____

Date: _____

ATTACHMENT A

<u>DATA REQUEST FORM</u>

This Data Request Form contains the specific terms and requirements of a specific Data sharing request.

<u>To Be Completed By the Requesting Entity</u>:

1. Disclosing Entity (Entity Name):

2. Information Coordinator:

3. Requesting Entity:

4. Information Coordinator:

5. Data Requested:

6. Permitted Uses:

7. How Often Will This Data Be Needed?:
   One Time ☐
   Periodically ☐
        Daily ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Annually ☐
   Near Real Time ☐
   Real Time ☐

8. Requested Users: See Attachment 1

9. | Requested Date of Completion:

Requesting Entity Signature

First/Last Name:

Signature:

Title:

Date:

To be completed by the Disclosing Entity:

10. | This Request is hereby:
☐ Approved in full
☐ Denied in its entirety, or in part with respect to_____, due to:

    ☐ No legal authority

    ☐ Reputational/Operational Risk

    ☐ Security Risk
    ☐ Do not possess the Data requested
    ☐ Other: _____

If the Request was Approved, please complete the following:

11. | Agreed Method of Transmission / Specific Transfer Requirements:

12. | Confidentiality Requirements or Security Protocols: [attach additional pages as necessary]

13. | Description of Records and Data to Be Disclosed: [attach additional pages as necessary]

14. | Risk or Inspection Requirements: [attach additional pages as necessary]

15. | Data Destruction Requirements: [attach additional pages as necessary]

16. | Authorized Persons and Staff: [attach additional pages as necessary]

17. | Requested Date of Completion:

Disclosing Entity Signature

First/Last Name:

Signature:

Title:

Date:

ATTACHMENT B

<u>INFORMATION COORDINATORS</u>

<u>BCAD</u>
BCAD Information Coordinator: Yesica Antu-Sanchez
Email: rmo@bcad.org
Work Phone: 210.242.2501

<u>CoSA</u>
CoSA Information Coordinator: Naji Tabet
Email: naji.tabet@sanantonio.gov
Work Phone: 210.207.8748

<u>CPS Energy</u>
CPS-E Information Coordinator: TBD
Email: kabirkelbach@CPSEnergy.com
Work Phone: 210.353.2283

<u>SAHA</u>
SAHA Information Coordinator: Ronald Scott Glover
Email: Ronald_Scott_Glover@saha.org
Work phone: 210.477.6604
Business cell: 210.559.7371

<u>SARA</u>
Alexander Rodriguez
Email: arodriguez@sara-tx.org
Work Phone: 210.302.3699
Physical Address: 100 E Guenther St. San Antonio TX 78204

<u>SAWS</u>
SAWS Information Coordinator: Maxim Mokeyev
Email: maxim.mokeyev@saws.org
Work phone: 210.233.3458

<u>VIA</u>
VIA Information Coordinator: Lesa Chilton
Email: lesa.chilton@viainfo.net
Work Phone: 210.362-2309

EACH ENTITY RESERVES THE RIGHT TO UPDATE THE INFORMATION COORDINATOR.

ATTACHMENT C

PERSONS AND ADDRESSES FOR NOTICE

BCAD
Paul Thepuatrakul, Information Systems Director
Email: pthepuatrakul@bcad.org
Work Phone: 210.242.2513
Physical Address: 411 N Frio St., San Antonio, TX 78207

CoSA
Craig Hopkins, Chief Information Officer
Email: craig.hopkins@sanantonio.gov
Work Phone: 210.207.7907
Physical Address: 111 Soledad St., San Antonio, TX 78205

CPS Energy
 (Will be our legal team)Work Phone: 210.353.2283
Business Cell: 210.483.3108
Physical Address: 145 Navarro, MS 100902, San Antonio,TX 78205

SAHA
Jo Ana Alvarado, Director of Innovative Technology
Email: joana_alvarado@saha.org
Work phone: 210.477.6602
Business cell: 210.861.5963
Physical Address: 818 S. Flores, San Antonio, TX 78204

Ronald Scott Glover, Manager of Software Development
Email: Ronald_Scott_Glover@saha.org
Work phone: 210.477.6604
Business cell: 210.559.7371
Physical Address: 818 S. Flores, San Antonio, TX 78204

SARA
Alexander Rodriguez, Information Technology Manager
Email: arodriguez@sara-tx.org
Work Phone: 210.302.3699
Physical Address: 100 E Guenther St. San Antonio, TX 78204

SAWS
Maxim Mokeyev, Executive Management Analyst
Email: maxim.mokeyev@saws.org
Work Phone: 210.233.3458
Physical Address: 2800 US Hwy 281, San Antonio, TX 78212

<u>VIA</u>
Steve Young, Vice President of Information Technology
Email: steve.young@viainfo.net
Work Phone: 210.362.2270
Physical Address: 800 W. Myrtle, San Antonio, TX 78015

ATTACHMENT D

<u>CONFIDENTIALITY AGREEMENT FORM</u>

I, the undersigned, hereby acknowledge that I have been provided a copy of the Agreement between the Disclosing Entity and the Entity I work for or represent, including the relevant Data Request Form(s), and that use or disclosure of any Confidential Information for any unauthorized purpose constitutes grounds to immediately revoke my access to the Confidential Information. I also agree that I will:

(a)   use Confidential Information of a Disclosing Entity only for the permitted uses specified in the relevant Data Request Form;

(b)   disclose Confidential Information of a Disclosing Entity only to Authorized Users who need access to such Confidential Information for the permitted uses specified in the Data Request Form and who are under written obligations of confidentiality, non-use, and non-disclosure to the Disclosing Entity on terms substantially similar to those imposed in this Agreement (Interlocal Data Sharing Agreement) (or, in the case of accountants and attorneys, are bound by professional obligations of confidentiality);

(c)   ensure that the Confidential Information of a Disclosing Entity is protected from unauthorized use, reproduction and disclosure in accordance with the requirements of the Agreement and the relevant Data Request Form(s), and by using no less than the same degree of care as I am required to use for the confidential information of mine, my client, or my employer; and

(d)   promptly notify my supervisor and the Information Coordinator of any circumstances that would cause me to believe that Confidential Information has been, or may be in jeopardy of being, accessed by unauthorized parties or used in ways that are not permitted by the Agreement or the relevant Data Request Form.
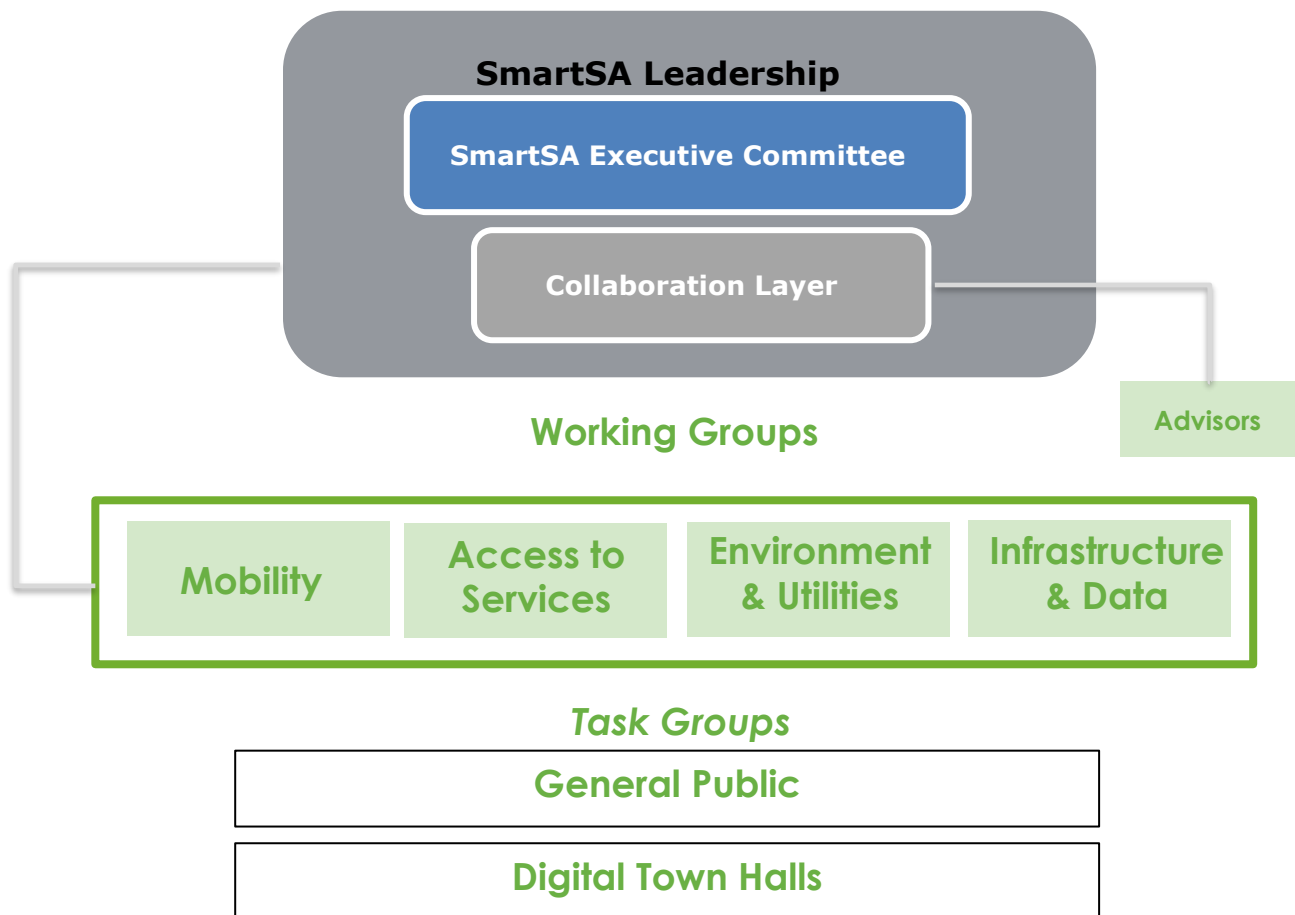
Signature of Employee:

Printed Name:

Name of Supervisor:

Name of Entity:

ATTACHMENT E

SMARTSA GOVERNANCE STRUCTURE

SmartSA Leadership

SmartSA Executive Committee

Collaboration Layer

Working Groups

Advisors

| Mobility | Access to Services | Environment & Utilities | Infrastructure & Data |

Task Groups

General Public

Digital Town Halls

SmartSA Executive Committee	The ExCo will provide leadership and insights, funding, branding direction, policy direction and decision rights as owners of assets.
Collaboration Layer	Comprised of the six Chief Information Officers from each organization will ensure consistency with the following elements: accountability and prioritization of projects, master planning, resource sharing and communications.
Advisors	The purpose of SmartSA Advisors is to provide perspective & insights to the Collaboration Layer. This group is comprised of organizations in the public sector, private sector and research institutions.
Working Groups	The Working Groups will be responsible for developing and executing project plans for approved SmartSA projects.

109729987\V-5