MEMORANDUM OF UNDERSTANDING BETWEEN TRAVIS COUNTY AND THE CITY OF AUSTIN FOR THE AVOIDANCE OF DUPLICATION OF BENEFITS REGARDING THE IMPLEMENTATION OF THE EMERGENCY RENTAL ASSISTANCE PROGRAM

This Memorandum of Understanding for the Avoidance of Duplication of Benefits Regarding the Implementation of the Emergency Rental Assistance Program ("Agreement") is entered into by and between Travis County, a political subdivision of the State of Texas ("County") and the City of Austin, a municipal corporation and political subdivision of the State of Texas ("City") (each a "Party" and collectively, the "Parties").

Recitals

The U.S. Congress has enacted numerous measures to assist those affected both directly and indirectly by the Coronavirus Disease 2019 ("COVID-19"). On December 27, 2020, the President of United States signed into law the Consolidated Appropriations Act of 2021, which included the Coronavirus Response and Relief Supplemental Appropriations Act of 2021 (section 501 of Division N of the Consolidated Appropriations Act, 2021, Pub. L. No. 116-260 (Dec. 27, 2020) (the "Act"). The legislation included $25 billion in additional money for state and local governments to provide rent and utility assistance to eligible households through December 31, 2021.

County received an allocation of $10.7 million, administered by the U.S. Department of Treasury for the purposes of implementing the Emergency Rental Assistance program described in the Act ("ERAP") within the County's jurisdiction.

City received an allocation of $29,578,788 million from the U.S. Department of the Treasury in order to implement ERAP in its jurisdiction.

In accordance with ERAP rules, County and City must avoid a duplication of benefits to ERAP program beneficiaries in their respective jurisdictions. The Parties, therefore, will enter into a data sharing agreement whereby each Party will share certain data elements for such purpose.

In addition to entering into a data sharing agreement, the Parties also desire to establish a process described in this Agreement to avoid the duplication of benefits to program beneficiaries whereby each Party has certain roles and responsibilities.

In providing each other with data connected with ERAP, both Parties must establish and comply with data privacy and security requirements as stated in section 501(g)(4) of Division N of the Act as follows:

> (i) include appropriate measures to ensure that the privacy of the individuals and households is protected;
> (ii) provide that the information, including any personally identifiable information, is collected and used only for the purpose of submitting reports required under section 501(g)(1) of the Act; and
> (iii) provide confidentiality protections for data collected about any individuals who are survivors of intimate partner violence, sexual assault, or stalking.

Now, therefore, County and City agree as follows:

Agreements

1.0 Purpose. The purpose of this Agreement is for the County and City to share limited information about the recipients of ERAP funding for the purpose of avoiding a duplication of benefits in accordance with section 501(g)(4) of Division N of the Act.

2.0 County will:

2.1 Produce and provide to the City, or an entity(ies) with which City contracts for the implementation of the City's ERAP program ("City Contractor"), a duplication of benefits data file indicating those households that have been approved for payment of Emergency Rental Assistance benefits from the County's allocation.

2.1.1 The duplication of benefits data file will be in comma-separated format and will be provided to the City, or City Contractor, via a secure file transfer protocol (sFTP), and will contain the following data elements in connection with a household that has been approved for payment of Emergency Rental Assistance benefits from the County's allocation:

- Unique Applicant ID (Confirmation ID)
- First Name
- Last Name
- Address 1
- Address 2
- City
- State
- Zip
- Month 1 receiving benefit
- Payment amount for Month 1
- (additional Months and Amounts, as applicable)

2.2 Be responsible for recouping funds paid to a household for which the City has already made payment to the household, provided that both of the following are true:

- The City has included the household on a City duplication of benefits data file prior to the County making payment for the same household; and
- Such household is located outside of the geographic boundaries of the City of Austin.

2.2.1 Other scenarios will be evaluated and resolved by the Parties on a case-by-case basis.

2.3 Legally bind County Contractor to all of the terms and conditions of the Data Sharing Agreement between the Parties regarding the Data Sharing Agreement attached to this Agreement as Exhibit 1.

3.0 City will:

3.1 Produce and provide to the County, or an entity(ies) with which County contracts for the implementation of the County's ERAP program ("County Contractor"), a duplication of benefits data file indicating those households that have been approved for payment of Emergency Rental Assistance benefits from the City's allocation.

3.1.1 The duplication of benefits data file will be in comma-separated format and will be provided to the County, or County Contractor, via a secure file transfer protocol (sFTP), and will contain the following data elements in connection with a household that has been approved for payment of Emergency Rental Assistance benefits from the City's allocation:

- Unique Applicant ID (Confirmation ID)
- First Name
- Last Name
- Address 1
- Address 2
- City
- State
- Zip
- Month 1 receiving benefit
- Payment amount for Month 1
- (additional Months and Amounts, as applicable)

3.2 Through City Contractor, provide a secure file transfer protocol (sFTP) directory for the sharing of files between the City and County.

3.3 Be responsible for recouping funds paid to a household for which the County has already made payment to the household, provided that the following is true:

- The County has included the household on a County duplication of benefits data file prior to the City making payment for the same household.

3.3.1 Other scenarios will be evaluated and resolved by the Parties on a case-by-case basis.

3.4 Legally bind City Contractor to all of the terms and conditions of the Data Sharing Agreement between the Parties regarding the Data Sharing Agreement attached to this Agreement as Exhibit 1.

4.0 Governing Law. This Agreement shall be interpreted, construed, and governed according to the laws of the State of Texas and is performable in Travis County, Texas.

5.0 Dispute Resolution. The Parties shall attempt to resolve any controversy, dispute or disagreement arising out of or relating to this Agreement, or breach thereof, by mediation, which shall be conducted in Travis County, Texas.

6.0 Termination of Agreement. Subject to Section 7.1 of this Agreement, this Agreement may be terminated at any time by either Party by providing the other Party with thirty (30) days' written notice. Unless terminated by written notice, this Agreement will terminate if either Party no longer provides disbursements to or on behalf of their respective ERAP program beneficiaries.

7.0 Miscellaneous.

7.1 Surviving Terms. Termination of this Agreement shall not relieve either Party from the obligation to perform it duties through the effective date of such termination or to perform such obligations as will survive termination. The obligations which will survive termination of this Agreement include all provisions of this Agreement regarding "Successors and Assigns" as stated

in Section 7.6 and "Liabilities and Claims" as stated in Section 8.0 and "Ownership" as stated in Section 11.0 of this Agreement. In addition, the obligations which will survive termination of this Agreement include all provisions of this Agreement regarding information security or confidentiality of information, including but not limited to Sections 2, 3, and 5 of Attachment A.

7.2 Entire Agreement. This Agreement, including exhibits and attachments, sets forth the entire agreement and understanding between County and City as it relates to the subject matter hereof, and supersedes and merges all prior discussions.

7.3 Amendment. No modification or amendment to this Agreement, nor any waiver of any rights under this Agreement, will be effective unless in writing, signed by both Parties. It is acknowledged that no officer, agent, employee or representative of County has any authority to change the terms of this Agreement unless expressly granted that authority by the Commissioners Court under a specific provision of this Agreement or by separate action of the Commissioners Court.

7.4. Severability.

7.4.1 Each covenant set forth herein constitutes a separate agreement that is independently supported by good and adequate consideration and shall be severable from the other provisions of this Agreement.

7.4.2 In the event that any of the previous provisions contained in this Agreement shall be held to be invalid, illegal, or unenforceable, such invalidity, illegality, or unenforceability shall not affect any other provision thereof, and this Agreement shall be construed as if such invalidity or unenforceable provision was never contained herein.

7.5 Force Majeure. Neither Party shall be financially liable to the other Party for delays or failures to perform under this Agreement caused by force majeure (i.e. those causes generally recognized under Texas law as constituting impossible conditions). Such delays or failures to perform shall extend the period of performance until these exigencies have been removed. The Party seeking to avail itself of this clause shall endeavor to notify the other Party within five (5) days, unless notification is impractical under the circumstances, in which case notification shall be done in as timely a manner as possible.

7.6 Successors and Assigns. This Agreement is solely for the benefit of County and City, its successors and its assigns. Neither Party is authorized to sell, transfer, or convey its rights under this Agreement to any other person.

7.7 No Third-Party Beneficiaries. Nothing in this Agreement shall be considered or construed as conferring any right or benefit on a person not a party to this Agreement nor imposing any obligation of either Party hereto to persons not a party to this Agreement.

7.8 Waiver of Breaches and Defenses; Reservation of Rights.

7.8.1 The waiver by either Party of a breach or violation of any provision of this Agreement shall not operate as, or be construed to be, a waiver of any subsequent breach of the same or other provision hereof.

7.8.2 If any Party to this Agreement breaches this Agreement, the other Party shall be entitled to any and all rights and remedies provided for by Texas law and any applicable Federal laws or regulations. All rights of County and under this City are specifically reserved, and the exercise or failure to exercise any right or remedy in this Agreement by County or City shall not

preclude the exercise of any other right or remedy under this Agreement or under any law, nor shall any action taken or not taken in the exercise of any right or remedy be deemed a waiver of any other rights or remedies.

7.8.3 It is expressly understood and agreed by the Parties that, neither the execution of this Agreement, nor any conduct of any representative of County or City relating to this Agreement, shall be considered to waive, nor shall it be deemed to have waived, any immunity or defense that would otherwise be available to it against claims arising in the exercise of its governmental powers and functions, nor shall it be considered a waiver of sovereign immunity to suit.

8.0 Liabilities and Claims Notification.

8.1 Liabilities and Claims. County shall not be liable for any claims, damages, or attorney's fees arising from any negligent or unlawful acts of the City or its employees in relation to this Agreement. City shall not be liable for any claims, damages, or attorney's fees arising from any negligent or unlawful acts of the County or its employees in relation to this Agreement. The Parties acknowledge that each entity is otherwise responsible for any claims or losses from personal injury or death or property damage that were caused by the acts or omissions of that entity, its agents, employees or representatives in the performance of the services and activities pursuant to this Agreement.

8.2 Claims Notification. If either Party receives notice or becomes aware of any claim, or other action, including proceedings before an administrative agency, which is made or brought by any person, firm, corporation, or other entity against itself or the other Party, that Party shall give the other Party written notice within three (3) days of being notified of this claim or threat of claim. Such notice shall include: written description of the claim; the name and address of the person, firm, corporation or other entity that made or threatened to make a claim, or that instituted or threatened to institute any type of action or proceeding; the basis of the claim, action or proceeding; the court or administrative tribunal, if any, where the claim, action or proceeding was instituted; and the name or names of any person against whom this claim is being made or threatened. This written notice shall be given in the manner provided in this Agreement. Except as otherwise directed, that Party shall furnish to the other Party copies of all pertinent papers received by it with respect to these claims or actions.

8.3 Notices. Any notices required or permitted hereunder shall be addressed to:

Travis County
Sherri E. Fleming, County Executive
Travis County Health and Human Services
P. O. Box 1748
Austin, Texas 78767

City:
Rosie Truelove, Director
Housing and Planning Department

P.O. Box 1088
Austin, Texas 78767

Notice to either Party shall be deemed received upon personal delivery or if sent by certified or registered mail, five (5) days after the date of mailing.

9.0 Warranties. **NEITHER PARTY MAKES ANY REPRESENTATION OR WARRANTY THAT THE DATA PROVIDED BY DISCLOSING PARTY WILL BE TIMELY, CORRECT, OR COMPLETE. NEITHER PARTY MAKES ANY EXPRESS, IMPLIED OR STATUTORY WARRANTIES REGARDING THE DATA PROVIDED UNDER THIS AGREEMENT. ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY OF THE DATA, OR NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. THE DATA MADE AVAILABLE BY PARTIES THROUGH THIS AGREEMENT IS PROVIDED "AS IS" AND "AS AVAILABLE."**

10.0 Calculation of Days. Any reference to "days" in this Agreement shall mean business days.

11.0 Ownership. Each Party retains ownership of the information it creates in performance of this Agreement ("Agreement Information"). Each Party is responsible for maintaining the privacy and security of its own Agreement Information.

12.0 Data Privacy and Security Requirements. In sharing the data elements described in this Agreement, the Parties will comply with the Data Privacy and Security Requirements attached to this Data Sharing Agreement as Attachment A.

13.0 Public Purpose. By execution of this Agreement, the Parties hereby find that the act of establishing a process to avoid a duplication of benefits under the terms of this Agreement constitutes a significant public benefit, positively impacting members of the population which the Parties serve. The Parties further find that the act of establishing a process to avoid a duplication of benefits will advance the public purpose of complying with the program rules established by the U.S. Department of the Treasury.

14.0 Duplicate Originals. This Agreement will be executed in duplicate originals and will be effective when executed by both Parties.

[Signature Page to Follow]

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

TRAVIS COUNTY

DocuSigned by:
Andy Brown
C21317DB291D47D...

Andy Brown
Travis County Judge

6/30/2021
Date

CITY OF AUSTIN

DocuSigned by:
7EB23E7D8D5D41D...

Rosie Truelove
Director, Housing and Planning Department

7/15/2021
Date

Exhibits and Attachments

1. Attachment A (Data Privacy and Security Requirements)

Attachment A
Data Privacy and Security Requirements

1. **Definitions**:

"Authorized Personnel" means a Party's employees, agents or representatives: (1) who have a need to know or otherwise access the other Party's Confidential Information to enable that Party to perform its obligations under this Agreement; (2) whose identities have been disclosed to the Party and have been approved by the other Party to provide services or perform Party obligations under this Agreement; and (3) have agreed in writing to be bound by the provisions of the Agreement, including but not limited to all provisions regarding information security or confidentiality of information.

"Breach of Security" or "**Breach**" means the actual or suspected unauthorized acquisition, accessing, modification, or disclosure of **Confidential Information** that compromises the security, confidentiality, or integrity of such information, including data that is encrypted if the person accessing the data has the key required to decrypt the data.[1]

"Confidential Information" means, with respect to either Party, any Information that includes confidential or sensitive information of any kind, including but not limited to criminal justice information, federal tax information, personally identifying information, protected health information, or sensitive personal information.

"Information" means, with respect to either Party, any data or information owned by such Party or in its actual or constructive possession, and any documents related thereto.

"Personal Identifying Information" or **"PII"** means information that alone, or in conjunction with other information, identifies an individual.

"Sensitive Personal Information" or **"SPI"** means the information described in the Texas Identity Enforcement and Protection Act (Tex. Business & Commerce Code Chapter 521), including: (1) an individual's first name or first initial and last name, together with one or more of the following: (a) the individual's social security number; (b) the individual's driver's license number or government-issued ID number; or (c) the individual's bank account number or debit or credit card number and security code, password, or access information; or (2) any information that identifies an individual and relates to the individual's physical or mental health, the provision of health care, or payment for the provision of health care.

2. **Security and Privacy Compliance**
    a. Each Party shall keep the other Party's Confidential Information received under the Agreement and any documents related thereto strictly confidential.
    b. The Parties shall comply with all applicable federal, state, and local privacy and data protection laws, as well as all other applicable regulations and directives.
    c. Each Party shall implement administrative, physical, and technical safeguards to protect the other Party's Confidential Information that are no less rigorous than accepted industry practices including, but not limited to, the guidelines in the most recent version of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. All

such safeguards shall comply with applicable federal and state privacy and data protection and privacy laws.

d. If applicable, each Party will legally bind any subcontractors to the same requirements stated herein and in the Agreement. Each Party shall ensure subcontractors impose these same requirements to any subcontractor of the Party's subcontractor(s).
e. Neither Party will share the other Party's Confidential Information with any third parties unless it has received the other Party's express prior written permission.
f. Each Party will ensure that initial privacy and security training that is appropriate to the subject matter of the Agreement and is acceptable to the other Party, in its sole discretion, and annual training thereafter, is completed by its employees or subcontractors, if applicable that have access to the other Party's Confidential Information or who create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle the other Party's Confidential Information on behalf of the other Party. Each Party agrees to maintain and, upon request, provide documentation of training completion, or other mutually acceptable documentation, to the other Party.

3. **Information Ownership**
   a. Each Party shall retain full ownership of all its own Information, including all Confidential Information of such Party, provided to the other Party or to which the other Party otherwise gains access.
   b. Upon termination of the Agreement, each Party shall promptly return to the other Party all of the other Party's Information that is in the possession of the returning Party or its agents or subcontractors, if applicable. Neither Party shall retain copies or back-up records of any of the other Party's Information. The obligations set forth in this Attachment with respect to Confidential Information of either Party shall survive termination of the Agreement. Each Party shall refrain from any further use and disclosure of any Confidential Information if and to the extent the return of the other Party's Confidential Information is infeasible. If such return is infeasible, as mutually determined by the Parties, a Party may direct the other Party to destroy any of its Confidential Information in the other Party's possession. Any such destruction shall be verified by the Parties.

4. **Data Mining**
   a. Neither Party shall use the other Party's Information for any purpose not expressly authorized in writing in advance by the owner of such Information. Each Party agrees to take all physical, technical, administrative, and procedural measures reasonably necessary to ensure that no unauthorized use of the other Party's Confidential Information occurs.

5. **Breach of System Security**
   a. As a condition of the Agreement and prior to its effective date, each Party will provide to the other Party the name and contact information of a designated representative of the Party who shall serve as the Party's primary information security contact. This individual will serve as the Party's single point of contact on all information security matters that may arise under the Agreement, and will communicate with the other Party's Information Security department as often is reasonably necessary or appropriate to ensure that all of the other Party's Confidential Information is protected against unauthorized access, modification, use or disclosure.
   b. Upon discovery of a Breach of Security or suspected Breach of Security by a Party ("Discovering Party"), the Discovering Party agrees to notify the other Party as soon as

possible upon discovery of the Breach of Security or suspected Breach of Security, but in no event shall notification occur later than 24 hours after discovery. Within 72 hours, the Discovering Party agrees to provide, at minimum, a written preliminary report regarding the Breach or suspected Breach to the other Party with root cause analysis including a log detailing the data affected. The Discovering Party agrees to fully cooperate with any investigation to determine if a Breach of Security has occurred and to what extent.

c. In addition to notifying the other Party, the Discovering Party agrees to also make notifications in the manner required in the PCI DSS requirements and applicable laws.
d. Upon discovery of a suspected or actual Breach of Security, the Discovering Party will not alter or destroy any related records and will maintain complete and accurate documentation regarding any modifications made to the records.
e. The Discovering Party agrees to take all reasonable steps to immediately remedy a Breach of Security and prevent any further Breach of Security.
f. A Party whose actions or failure to act caused a Breach of Security ("Breaching Party") shall be required to provide notification of a Breach of Security immediately to both the other Party ("Non-breaching Party") and all persons who may be adversely affected by such breach (subject to the Breaching Party's obligation to notify the Non-Breaching Party as described in this Attachment), or as soon as is reasonably possible under the circumstances, but in no event later than is required in accordance with applicable law.
g. A Discovering Party or Breaching Party shall not inform any third party of any Breach of Security or suspected Breach of Security without obtaining the other Party's prior written consent unless required to do so by law or industry regulation.
h. If the Breach of Security includes Sensitive Personal Information, such as social security numbers, payment card information, or health information, the Breaching Party will provide all affected individuals with access to one (1) year of credit monitoring services at no cost to the Non-breaching Party or the affected individuals.
i. A Breaching Party will be liable for all damages or expenses that may be incurred by the Non-breaching Party as a result of the Breach of Security, subject only to any express limitation of liability that may be set forth in the Agreement.

6. **Right to Audit**
   a. Upon a Party's request ("Requesting Party") and to confirm the other Party's ("Non-requesting Party") compliance with this Attachment, the Non-requesting Party will grant to the Requesting Party, or to such Party's authorized agent or representative, permission to perform an assessment of the Non-requesting Party's books, records, operations or facilities as they may reasonably pertain to the other Party's performance (or if applicable, to its agents' or subcontractors' performance) of such Party's obligations under this Agreement, particularly with regard to Confidential Information. The Non-Requesting Party agrees to fully cooperate with such assessment, audit, examination, investigation, or review by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that stores, processes, or transports the Requesting Party's Confidential Information. In lieu of such an assessment, audit, examination, investigation, or review, a Non-requesting Party may supply, upon the Requesting Party's approval, the following reports: SSAE16, ISO/ICE 27001 Certification, FedRAMP Certification, SOC 2 Type II, and PCI Compliance Report. Each Party shall ensure that this clause concerning both Parties' authority to assess, audit, examine, investigate, or review is included in any subcontract it awards, if applicable.

b. At the request of the other Party, each Party agrees to promptly and accurately complete a written information security questionnaire provided by the Requesting Party regarding the Non-requesting Party's business practices and information technology environment in relation to the Requesting Party's Confidential Information.
c. Notwithstanding the Parties' obligations to each other described under this Section, neither Party shall be required to disclose to the other Party any information that it reasonably determines would compromise the security of its own technology, networks, systems, or premises or that would cause it to adversely affect or breach its obligations of confidentiality to its other clients, provided that it reasonably cooperates with the Requesting Party to provide responsive information in a manner that minimizes or avoids its security concern.

7. Business Continuity Requirements for the Parties or Third-Party Data Hosting

a. The Parties shall maintain appropriate business continuity plans and procedures for their respective systems, whether hosted by themselves or a third party, to ensure security of all Information in the event of a disruption, disaster, or failure of either Party's primary data systems.
b. Each Party will notify the other Party of any unanticipated disruption in the performance of its obligations under the Agreement and will provide regular updates on the workaround being implemented to mitigate disruption and resolve the issue.
c. The implementation of a Party's Business Continuity Plan workarounds will be at no additional cost to the other Party.
d. The Parties will perform regular backups of their respective systems and ensure all backups are successfully completed.
e. The Parties will test their respective planned workarounds to services at least once in every twelve months in a controlled environment and will promptly implement lessons learned identified from the test and update the Business Continuity and/or Disaster Recovery Plan accordingly.