TDHCA Information Security and Privacy Agreement

This agreement ("ISP Agreement") is entered into by the Texas Department of Housing and Community Affairs, an official agency of the State of Texas ("Department"), and _____[name of entity]_____, a __[State and corporate form, e.g. "Texas Limited Liability Corporation" etc.]_____ ("Contractor"). The purpose of the agreement is to ensure the security and privacy of Protected Information belonging to persons who do business with the Department. Department Contractors are required to comply with all security and privacy measures herein. The scope and complexity of each Contractor's specific security and privacy measures will vary depending on the size of the organization and risks presented by Contractor's operations. This agreement is effective on the date it is fully executed by the parties.

A. Definitions

The following words and terms, when used in this Agreement, have the following meanings unless the context clearly indicates otherwise.

"Computing Device" means any personal computer, laptop, server, smart phone, or any other data processing device that is used to connect to the Department's Network. (Note: Connecting to the Agency's network means accessing or logging into any internal Agency system, application, or resource. This includes use of TDHCA software applications such as CMTS. It does not include activities that do not require access to internal systems, such as simply sending an email to the Agency.)

"Contractor" means a third party, including, but not limited to, outside auditors and legal counsel, funding agencies, Vendors or Subrecipients, including any of their Representatives that may gain access to Protected Information on account of a contract with the Department.

"Criminal History Records Information" – means, for the purposes of TEX. GOV'T. CODE §411, information collected about a person by a Criminal Justice Agency that consists of identifiable descriptions and notations of arrests, detentions, indictments, information, and other formal criminal charges and their dispositions. The term doesn't include (i) identification information, including fingerprint records, to the extent that the identification information does not indicate involvement of the person in the criminal justice system; or (ii) driving record information under Subchapter C, Chapter 521 Transportation Code.

"Department" means the Texas Department of Housing and Community Affairs.

"Department's Network" includes all systems, infrastructure, and services the Department uses to store, process, or transmit data. This typically includes:

- Wired and wireless networks (internal and external connections)
- Servers and cloud services used by the Department

- Network equipment such as routers, switches, and firewalls
- Department-managed applications and databases
- Remote access systems, such as VPNs or secure portals

"Financial Statements of a Tax Credit Applicant" means, for purposes of TEX. GOV'T. CODE §2306.6717(d)(Public Information and Hearings), a formal statement of the financial activities of a Low Income Housing Tax Credit Applicant, submitted to the Department as part of a Low Income Housing Tax Credit Application, including but not limited to, the balance sheet, income statement, cash flow statement or changes in equity.

"Information Resources" means the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

"ISP Agreement" means this agreement.

"Non-Public Personal Information" means, for purposes of the Graham-Leach-Bliley Act (15 USC §§6801-6809 and 6821-6827), and implementing regulations, personally identifiable financial information provided by an individual in connection with applying for or receiving a financial product or service, unless the information is otherwise publically available.

"Personal Identifying Information" means, for purposes of TEX. BUS. & COM. CODE Chapter 521 (Unauthorized Use of Identifying Information), and any implementing regulations, information that alone or in conjunction with other information identifies an individual, including an individual's name, Social Security number, date of birth, or government-issued identification number, mother's maiden name, unique biometric data including fingerprint, voice print, retina or iris image, unique electronic identification number, address, or routing code, and telecommunication access devices as defined by TEX. PENAL CODE §32.51.

"Personal or Business Financial Information" means, for purposes of TEX. GOV'T. CODE §2306.039 (Open Meetings and Open Records), any personal or business financial information including, but not limited to, Social Security numbers, tax payer identification numbers, or bank account numbers submitted to the Department to receive a loan, grant, or other housing assistance by a housing sponsor, individual or family.

"Protected Information" means Criminal History Records Information, Financial Statements of a Tax Credit Applicant, Non-Public Personal Information, Personal Identifying Information, Personal or Business Financial Information, Protected Health Information, Sensitive Personal Information, or Victims of Violence Information, and WAP Applications and Participation Information.

"Prohibited Technologies" refers to TikTok and any additional hardware or software products identified in Department's Prohibited Technologies Security Policy (SOP 1264.07) and any additional hardware or software products added to this Policy and identified by the State Department of

Information Resources ("DIR"). DIR is maintaining a list of prohibited hardware and software at https://dir.texas.gov/information-security/prohibited-technologies.

"Protected Health Information" has the meaning ascribed to it in 45 CFR §160.103. Generally, it includes any information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

"Representative" means any officer, employee, contractor, subcontractor, member, director, advisor, partner, or agent of a Contractor, or any person serving in such a role, however titled or designated.

"Sensitive Personal Information" means, for purposes of TEX. BUS. & COM. CODE Chapter 521 (Unauthorized Use of Identifying Information), 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 items are not encrypted: (1) social Security number, (2) driver's license or government-issued identification number, (3) account or credit/debit card number in combination with any required security code, access code, or password that would permit access, or (4) information that identifies or reveals an individual and the physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual. The term does not include publicly available information that is lawfully made publicly available.

"Subrecipient" An organization with whom the Department contracts, and entrusts to administer federal or state program funds, including but not limited to, units of local government, non-profit and for-profit corporations, administrators, community action agencies, collaborative applications, sub-grantees, NSP developers, land banks, participating mortgage lenders and non-profit owner-builder housing providers.

"Vendor" means a person or organization that supplies goods or services, properly procured under relevant laws, to the Department.

"Victims of Violence Information" means any information submitted to a covered housing provider, including the Department and its Contractors pursuant to 24 CFR §5.2007, including the fact that an individual is a victim of domestic violence, dating violence, sexual assault, or stalking. For HOME ARP this also includes victims of human trafficking. Also included pursuant to Tex. Gov't Code §552.138 is information regarding the location or physical layout, an employee, volunteer, former or current client, or the provision of services to a former or current client, a private donor, or a member of a board of directors or board of trustees of a family violence shelter center, victims of trafficking shelter center, or sexual assault program.

"WAP Applications and Participation Information" means, for purposes of Weatherization Program Notice 24-1, U.S. Department of Energy, issued November 17, 2023, or subsequent notice concerning the same subject matter regarding the Department of Energy Weatherization Assistance Program ("WAP"), any specifically identifying information related to an individual's eligibility

application for WAP or the individual's participation in WAP, such as name, address, or income information.

B. Security Measures for Devices that Connect to Department Network

Any third-party Computing Device that is used to connect to the Department's internal network either physically or through a Virtual Private Network ("VPN") must meet the following requirements:

1. Contractor shall not access Department's networks with its own equipment unless (a) the equipment meets Department's security standards described herein, and (b) the Department has approved the access in writing.

2. Department-licensed software shall not be installed on a non-Department Computing Device unless explicitly permitted by the licensor and authorized in writing by the Information Systems Director for the Department.

3. Contractor shall not access any area of Department premises except those specific areas for which Contractor has been given written permission by the Department.

4. Contractor shall ensure that any Computing Device that is connected to the Department network is compliant with all Department hardware, software, and security standards. This includes anti-virus software running the latest virus definition patterns and any critical security patches required to protect the device from outside vulnerabilities.

5. Contractor shall ensure that any of its Computing Devices remotely connected to the Department's network through VPN are not connected to any other external networks through VPN at the same time. Reconfiguration of any Contractor Computing Device that connects to the Department network for the purpose of split-tunneling or dual homing (multiple network cards) is not permitted.

6. Access to the Department's network shall only be granted for a period of time agreed upon in writing by both parties, however the period may be terminated earlier at the sole discretion of the Department, which discretion shall not be unreasonably exercised, upon not less than twenty-four (24) hours' notice.

7. The Department shall not be responsible or liable for non-Department assets.

C. Security Measures for Maintenance of Department Protected Information External to the Department Network

Contractor and any Representative who maintains Protected Information in systems external to the Department network shall comply with the information technology (IT) security requirements defined below:

1. Contractor shall maintain an inventory of all IT assets, including all IT hardware, software, and data. The IT asset inventory shall be used in risk assessment activities and IT security policy development.

2. Contractor shall implement and maintain an IT risk management program in which risks are identified, documented, assessed, prioritized, controlled, and monitored.

3. Contractor shall ensure Protected Information is recoverable in accordance with its IT security policy.

4. Contractor shall adhere to monitoring techniques and procedures for detecting, reporting, and investigating security incidents.

5. Contractor shall provide IT security training to its employees upon hire and at a Contractor defined frequency, thereafter. The training shall include appropriate elements from the IT security policy, shall stress the importance of protecting Protected Information, shall include notice of consequences for noncompliance with policy, accidental loss of Protected Information, or misuse of Protected Information, shall cover procedures for the proper disposal of Protected Information, and shall cover responding to security incidents and breaches. Contractor shall document all training and make the records available to the Department upon request.

6. Contractor shall conduct criminal background checks on its employees with access to Protected Information. Contractor shall make this information available to the Department upon request.

7. If Contractor performs software development on systems in which Protected Information is maintained, Contractor shall separate development and production environments and ensure that only staff with a need to update production data have this type of access. People who perform software development duties shall not have access to modify production data.

8. If Contractor performs software development on systems in which Protected Information is maintained, Contractor shall follow a software change control process, through which appropriate management approval shall be documented prior to the migration of software changes from development to production environments.

9. Contractor certifies with its signature, below, that it maintains and follows an IT security policy that has incorporated the below minimum standards before any work begins. The IT security policy shall address the following topics and subtopics, where applicable, based on the size and complexity of the organization:
   a. Account Management and Systems Access
   b. Application Security
      i. Configuration management for PCs, laptops, and servers
      ii. Network Security and intrusion prevention
      iii. Patch management for PCs, laptops, and servers
      iv. Protection of routers, switches, and other network devices
      v. Security of wireless networks and devices
      vi. Virus and malware protection
   c. Authorized equipment and software
   d. Backup, disaster recovery, testing, and continuity of operations
   e. Data classification
   f. Development or acquisition of Information Resources
   g. Encryption
   h. Handling and responding to security incidents
   i. Physical security
   j. Portable Computing Devices and Media
      i. Portable Computing Devices, including laptops, handheld computers, personal digital assistants, and cell phones
      ii. Portable media, including any removable discs, USB or other flash storage devices, hard drives, CDs, and DVDs
   k. Release and disposal of Information Resources
   l. Secure disposal of Protected Information
   m. Secure physical file transfer
   n. Secure electronic file transfer
   o. Security awareness and training for employees
   p. Testing and monitoring of the controls defined in the IT Security Policy

10. The following are specific requirements that shall be included in Contractor's IT security policy and shall be in effect for as long as Contractor retains any Protected Information.
   a. Contractor facilities shall be restricted to appropriate personnel using access restraints such as access cards or keys. Servers, network equipment, and backup media shall be maintained in locked, unlabeled facilities with access restricted to designated employees.
   b. For file security or file transfer requiring encryption, Contractor shall use 256-bit FIPS 140-2 or 140-3 approved security functions. For guidance, refer to FIPS Publications 140-2 or 140-3, *Security Requirements for Cryptographic Modules*, at https://csrc.nist.gov/publications/fips.

c. Portable Computing Devices or media containing Protected Information of individuals participating in Department programs or Department employees shall comply with the following requirements:

i. Portable computing devices shall be password protected. ii. Contractor shall not physically transport portable computing devices or media containing Protected Information of individuals participating in Department programs or Department employees outside of its facilities or from one facility to another without encrypting all Protected Information following the encryption requirement defined above. For definitions and guidance, refer to NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, at https://csrc.nist.gov/publications/sp.

d. Contractor shall not email Protected Information unless the information is encrypted following the encryption requirement defined above.

e. Contractor shall not use unencrypted Internet protocols, such as Hyper Text Transfer Protocol ("HTTP") or File Transfer Protocol ("FTP"), to transfer Protected Information over the Internet. Contractor shall use Secure File Transfer Protocol ("SFTP") with 256-bit encryption or better or HTTPS with Transport Layer Security ("TLS") [version 1.2 or later] with 256-bit encryption or better.

f. Contractor's password policy shall require the following elements: minimum length, combination of alpha and numeric or special characters, and password duration and rotation.

g. Contractor shall ensure that only software that has been evaluated and pre-approved by Contractor is installed on any of its Computing Devices or network devices.

h. If Contractor maintains servers that host applications or services accessible over the Internet, Contractor shall logically segment network resources and services, so that those intended for internal use only are separated into private IP networks and those intended to be accessible from the Internet are separated into public IP networks. Contractor shall at a minimum use firewall and access control list technologies so that only necessary Internet ports and services are open to appropriate network resources.

i. Contractor shall consult the Department regarding the transfer, sale, or disposal of all Computing Devices, network devices, and electronic media containing Protected Information and provide for sanitization of said information using industry best practices like those defined in NIST Special Publication 800-88 Rev. 1, *Guidelines for Media Sanitization*, at https://csrc.nist.gov/publications/sp. This paragraph 11(i), shall survive the expiration or termination of any or all agreements that Contractor has with the Department, including this Agreement, as long as Contractor has possession or control of any Protected Information.

j. Contractor shall take affirmative and verifiable steps to ensure that no devices that constitute, contain, or have installed any Prohibited Technologies are utilized in connecting with state technology infrastructure, or in the transmitting, reviewing, or storing of any Department or State communications or data.

11. The Department may provide assistance to Contractor upon request by sending an email request to tsupport@tdhca.state.tx.us .

12. If Contractor is a "financial institution" pursuant to 12 U.S.C. §1843(k), Contractor certifies by its signature, below, that it will adhere to and maintain the standards for safeguarding customer information as described in Title 16 C.F.R. Part 314, including the designation of a qualified individual responsible for overseeing, implementing, and enforcing the institution's information security program.

D. General Requirements

1. In the event of an actual or suspected breach involving Protected Information stored by the Contractor, Contractor shall promptly notify the Department no later than twenty-four hours after discovery of the incident. The Contractor will coordinate and cooperate fully with the Department in making all breach notifications and taking all actions required by law to effect the required notifications.

2. If Contractor receives a request pursuant to the Texas Public Information Act for Protected Information maintained by Contractor, Contractor shall notify the Department within three (3) days of the receipt of the request by forwarding the request to open.records@tdhca.state.tx.us

3. The Department does not share Non-Public Personal Information for any purposes except for the purposes described in 12 CFR §1016.14 (processing and servicing transactions) and §1016.15 (other exceptions). All other uses of Non-Public Personal Information by Contractor are prohibited, including, but not limited to, using Non-Public Personal Information for marketing purposes.

4. Upon reasonable notice, and during regular business hours, Contractor shall make available for copying or inspection by the Department, the Office of the Attorney General, or the State Auditor's Office (and the U.S. Secretary of Health and Human Services if Protected Health Information is involved), records kept by Contractor related to the execution of its obligations under this ISP Agreement.

5. This ISP Agreement is the parties' entire agreement on this subject and supersedes all prior or contemporaneous agreements. Any modifications to this ISP Agreement shall not be effective unless in writing and signed by both parties; provided, Department may amend this ISP Agreement, in its sole discretion in order to conform it to federal or state law.

6. Contractor shall ensure that only Representatives with a need to know will have access to any Protected Information and ensure that those Representatives read this ISP Agreement and comply with the requirements listed herein.

7. This ISP Agreement is not assignable or transferable by either party without prior written consent. Failure to enforce any provisions of this agreement will not constitute a waiver.

8. This ISP Agreement is governed by the laws of the State of Texas.

9. This ISP Agreement is effective on the date both parties have signed below and shall remain in effect so long as Contractor has access to Protected Information.

TO SHOW THEIR AGREEMENT, the parties have caused this ISP Agreement to be executed by their undersigned, duly authorized representatives on the dates below.

Contractor	**Texas Department of Housing and Community Affairs**
By: _____	**By:**_____
Printed Name: _____	**Printed Name:**_____
Title:_____	**Title:**_____
Date:_____ /_____/_____	**Date:**_____ /_____/_____