INVESTING IN COMMUNITIES

Sacramento Housing and Redevelopment Agency

And

Contractor: _____

Contract Confidentiality Requirement

Protecting Personally Identifying Information

The Sacramento Housing and Redevelopment Agency (SHRA) is federally funded and subject to the requirements of the federal Privacy Act of 1974 and various California statutes protecting privacy including the California State Constitution. Any contractor, vendor, business or person conducting business with SHRA, and has access to personally identifying information, is required to meet the standards outlined in the Privacy Act, and any Public and Indian Housing (PIH) Notice issued by the U. S. Department of Housing and Urban Development which is the regulating Agency of SHRA and all applicable state laws.

This document is an attachment to the contract effective _____ between SHRA and_____,(herein referred to as "Contractor"). This document spells out the requirements that must be met by the "Contractor," its sub-vendors, its employees, associates and persons who will have access to the Personally Identifying Information (PII) of a person who is/was an applicant to, current or former participant of any Housing Authority programs, or any current, past or future employee of SHRA.

DEFINITIONS:

Personally Identifying Information:

PIH Notice 2014-10 Privacy Protection Guidance for Third Parties: PII is defined as:

i) ". . . information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

ii) Sensitive Personally Identifiable Information. PII that when lost, compromised or disclosed without authorization could substantially harm an individual. Examples of sensitive PII include

social security or driver's license numbers, medical records, and financial account numbers such as credit or debit card numbers.

Privacy Act:

In accord with the Department of Justice, "The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements.

BASIC REQUIREMENTS:

The "Contractor" agrees to:

1. Comply with the requirements of the Privacy Act of 1974 and the requirement to protect PII as quoted from PIH Notice 2014-10 (and any subsequent PIH notices related to protecting PII that are released)
2. Impose the requirements of the Privacy Act of 1974 and PIH Notice 2014 and any subsequent notices on all of its employees, associates and persons who will have access to PII of a person who is/was an applicant, current or former participant of any Housing Authority programs, or any current, past or future employee of SHRA.
3. Participate in an initial and annual PII training to be conducted by SHRA or its assignee as a condition of the contract.
4. Immediately inform SHRA by phone AND through written notification when any section of this contract has been violated. Written notification must be sent to the appropriate Director and Program Manager for the program, and may be submitted by email.

CONTRACTOR'S AGREEMENT:

The "Contractor" agrees to:

i) Limit Collection of PII

(1) Not collect or maintain sensitive PII without proper authorization. Collect only the PII that is needed for the purposes for which it is collected.

ii) Manage Access to Sensitive PII

(1) Only share or discuss sensitive PII with those personnel who have a need to know for purposes of their work. Challenge anyone who asks for " access to sensitive PII for which you are responsible.

(2) Do not distribute or release sensitive PII to other employees, contractors, or other third parties unless you are first convinced that the release is authorized, proper and necessary.

(3) When discussing sensitive PII on the telephone, confirm that you are speaking to the right person before discussing the information and inform him/her that the discussion will include sensitive PII.

(4) Never leave messages containing sensitive PII on voicemail.

(5) Avoid discussing sensitive PII if there are unauthorized personnel, contractors, or guests in the adjacent cubicles, rooms, or hallways who may overhear your conversations.

(6) Hold meetings in a secure space (i.e., no unauthorized access or eavesdropping possible) if sensitive PII will be discussed and ensure that the room is secured after the meeting.

(7) Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII.

(8) Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.

iii) Protect Hard Copy and Electronic Files Containing Sensitive PII

(1) Clearly label all files containing sensitive PII by placing appropriate physical labels on all documents, removable media such as thumb drives, information systems, and application. Examples of appropriate labels might include ―For Official Use Only ‖ or ―For (Name of Individual/Program Office) Use Only. ‖

(2) Lock up all hard copy files containing sensitive PII in secured file cabinets and do not leave unattended.

(3) Protect all media (e.g., thumb drives, CDs, etc.,) that contain sensitive PII and do not leave unattended. This information should be maintained either in secured file cabinets or in computers that have been secured.

(4) Keep accurate records of where PII is stored, used, and maintained.

(5) Periodically audit all sensitive PII holdings to make sure that all such information can be readily located.

(6) Secure digital copies of files containing sensitive PII. Protections include encryption, implementing enhanced authentication mechanisms such as two- factor authentication and limiting the number of people allowed access to the files.

(7) Store sensitive PII only on workstations that can be secured, such as workstations located in areas that have restricted physical access.

iv) Protecting Electronic Transmissions of Sensitive PII via fax, email, etc.

(1) When faxing sensitive PII, use the date stamp function, confirm the fax number, verify that the intended recipient is available, and confirm that he/she has received the fax. Ensure that none of the transmission is stored in memory on the fax machine, that the fax is in a controlled area, and that all paper waste is disposed of properly (e.g., shredded). When possible, use a fax machine that uses a secure transmission line.

(2) Before faxing PII, coordinate with the recipient so that the PII will not be left unattended on the receiving end.

(3) When faxing sensitive PII, use only individually-controlled fax machines, not central receiving centers.

(4) Do not transmit sensitive PII via an unsecured information system (e.g., electronic mail, Internet, or electronic bulletin board) without first encrypting the information.

(5) When sending sensitive PII via email, make sure both the message and any attachments are encrypted.

(6) Do not place PII on shared drives, multi-access calendars, the Intranet, or the Internet.

v) Protecting Hard Copy Transmissions of Files Containing Sensitive PII

(1) Do not remove records about individuals with sensitive PII from facilities where SHRA information is authorized to be stored and used unless approval is first obtained from a supervisor. Sufficient justification, as well as evidence of information security, must been presented.

(2) Do not use interoffice or translucent envelopes to mail sensitive PII. Use sealable opaque solid envelopes. Mark the envelope to the person's attention.

(3) Do not allow employees, associates or persons to take PII documents home, but must return to the office of the "Contractor" or its Assignee

(4) When out in the field, PII information must be stored in the trunk

(5) PII Information must not be left in a car overnight.

(6) If any PII information must be transported by any mode of transportation, the PII information is secured and locked in the trunk of the vehicle or locked in a van. Files transported with PII information from the vehicle to the building must be in a sealed envelope or box. If information is being carried by a person it must be placed in a locked box.

(7) When using the U.S. postal service to deliver information with sensitive PII, double- wrap the documents (e.g., use two envelopes – one inside the other) and mark only the inside envelope as confidential with the statement ―To Be Opened By Addressee Only.

vi) Records Management, Retention and Disposition

(1) Follow records management laws, regulations, and policies applicable within your jurisdiction.

(2) Ensure all of the 'Contractor's' locations and all entities acting on behalf of the "Conrtractor" are managing records in accordance with applicable laws, regulations, and policies.

(3) Include records management practices as part of any scheduled oversight protocols.

(4) Do not maintain records longer than required.

(5) Destroy records after retention requirements are met.

(6) Dispose of sensitive PII appropriately – use cross-cut shredders or burn bags for hard copy records and permanently erase (not just delete) electronic records.

(7) The "Contractor should ensure that all of its employees, associates and persons who will have access to PII are familiar with reporting procedures.

vii) Promptly report all suspected compromises of sensitive PII related to the appropriate Director and Program Manager by phone AND in writing

PENALTIES FOR NON-COMPLIANCE:

SHRA Penalties: The contract to which this document is attached is subject to termination due to non-compliance or violation of either the Federal Privacy Act; the verified disclosure of PII or the failure to meet any of the requirements by the "Contractor" its employees, associates or persons within its agency. SHRA shall notify the "Contractor" in writing with at least 30 days notice of the contract termination

Civil Penalties: An individual can be held personally liable and may be fined up to $5,000 for each offense, or imprisoned up to five years or both for failing to comply with the regulations governing the use and unauthorized access to PII.

ACKNOWLEDGEMENT AND ACCEPTANCE:

I acknowledge all of the terms listed within this document and accept all of the requirements stated herein.

_____ _____

Contractor Name Contractor's Signature

_____

Date signed by Contractor

Ref: Contract effective: _____