CHICAGO HOUSING AUTHORITY
SOCIAL SECURITY NUMBER PROTECTION POLICY

POLICY AND PURPOSE

- This Policy establishes the requirements for compliance with the Illinois Identity Protection Act 5 ILCS 179/1 *et seq*. (the "Act"), to ensure the confidentiality and integrity of SSNs collected, maintained and used by the CHA. The goal of the Act's requirements that limit the collection, access and use of SSNs is to protect against the threat of identity theft.

- The Chicago Housing Authority ("CHA") Social Security Number ("SSN") Protection Policy ("Policy") establishes the recommended handling and protection procedures for CHA Board members, employees, consultants, contractors, residents and other authorized individuals with access to Personally Identifiable Information ("PII"), specifically, the social security numbers of CHA employees and residents.

- This Policy applies to all CHA employees, Board members, residents and other authorized individuals, regardless of funding sources. "Employee" or "Employees", hereinafter, when used alone, refers collectively to any CHA Board member, employee, consultant, contractor, resident and other authorized individual(s) having access to SSN information.

- This Policy will be strictly enforced. Any deviations by an Employee from the Policy must be justified in writing and approved by the Chief Executive Officer ("CEO") or the CEO designee.

SSN PROTECTION POLICY

I. Prohibited Activities.

a. General Prohibited Activities. No Employee may do any of the following:

i. Publicly post or publicly display in any manner an individual's SSN. "Publicly post" or "publicly display" means to intentionally communicate or otherwise intentionally make available to the general public.

ii. Print an individual's SSN on any card required for the individual to access products or services provided by the CHA.

iii. Require an individual to transmit a SSN over the Internet, unless the connection is secure or the SSN is encrypted.

iv. Print an individual's SSN on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery ("mail"), unless State or federal law requires the SSN to be on the document to be mailed. SSNs may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the SSN.

v. A SSN that is permissibly mailed will not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.

b. Additional Prohibited Activities. In addition, no Employee may do any of the following:

i. Collect, use or disclose a SSN from an individual, unless:

1. required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the SSN is otherwise necessary for the performance of the Employee's duties and responsibilities;

2. the need and purpose for the SSN is documented before or in connection with the collection of the SSN; and

3. the SSN collected is relevant to the documented need and purpose.

ii. Use the SSN for any purpose other than the purpose for which it was collected.

iii. Require an individual to use his or her SSN to access an Internet website.

c. Exceptions. The prohibitions noted in subsections I(a) and I(b) above do not apply to the following circumstances:

i. The disclosure of SSNs to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a

contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under the Act on a governmental entity to protect an individual's SSN will be achieved.

ii. The disclosure of SSNs pursuant to a court order, warrant, or subpoena.

iii. The collection, use, or disclosure of SSNs in order to ensure the safety of: State and local government employees including CHA employees; persons committed to correctional facilities, local jails, and other law-enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a State or local government agency facility including Employee facilities.

iv. The collection, use or disclosure of SSNs for internal verification or administrative purposes.

v. The disclosure of SSNs by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.

vi. The collection or use of SSNs to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.

II. Protections.

a. Limited Access. Only Employees who are required to use or handle information or documents that contain SSNs will have access.

b. Training. All Employees identified as having access to SSNs in the course of performing their duties shall be trained to protect confidentiality of SSNs. Training shall include instructions on the proper handling of information that contains SSNs from the time of collection through the destruction of the information.

c. Documentation and Authorization of Need. No Employee shall collect, store, use or disclose an individual's SSN unless authorized by the CEO or his designee.

d. Redacting. SSNs requested from an individual shall be provided in a manner that makes the SSN easily redacted if required to be released as part of a public records request.

e. Statement of Purpose(s). When collecting a SSN or upon request by the individual, a statement of purpose or purposes for which the CHA is collecting and using the SSN shall be provided.

f. Additional Protections. SSN information may not be maintained on a portable electronic device without the prior written approval of the CEO or his designee. SSN information may not be transmitted via e-mail unless encrypted in accordance with the requirements specified by the CEO or his designee.

III. Public Inspections and Copying of Documents.

Employees shall comply with the provisions of any other State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's SSN. In such cases, Employees shall redact SSNs from the information or documents before allowing the public inspection or copying of the information or documents.

IV. Compliance with Federal Law.

If a federal law takes effect requiring any federal agency to establish a national unique patient health identifier program, the CHA's compliance with federal law shall be deemed compliance with the Act and this Policy.

V. Embedded Social Security Numbers.

Employees shall not encode or embed a SSN in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, RFID technology or other technology, in place of removing the SSN.

VI. Authorization to Formulate Guidelines.

The CEO or his designee is authorized to issue guidelines for the effective implementation of the requirements of this Policy as it relates to SSNs collected by Employees.

VII. Compliance.

Failure to abide by this Policy or guidelines will subject Employees to discipline up to and including dismissal in accordance with the CHA's disciplinary policies.