TAUNTON HOUSING AUTHORITY EIV POLICY AND PROCEDURES

The Enterprise Income Verification System (EIV)

The EIV system is intended to provide a single source of income-related data to PHAs for use in verifying the income reported by tenants in the various assisted housing programs. The office of Public and Indian Housing (PIH) is responsible for administering and maintaining the EIV system.

Types of Upfront Verification of Income Provided by EIV

The EIV system compares the tenant income data obtained from various sources including:

Tenant-supplied income data captured on Form HUD-50059 and maintained in the PIC databases,

U.S. Department of Health and Human Services, National Directory of New Hires (NDNH) data. NDNH becomes the single source for wage, unemployment insurance benefit information, and the new hire (employment) information,

Social Security and Supplemental Security Income from the Social Security Administration (information formerly accessed through TASS); and

User profile information from the PIC database.

EIV Purpose

EIV data is the first level in the hierarchy of upfront income verification. The EIV data may be used in the following manner:

To verify a tenant's eligibility for continued participation in a HUD rental assistance program and to determine the level of assistance the tenant is entitled to receive.

*No adverse action can be taken against a tenant until the PHA has independently verified the EIV (according to the PHA's income verification policy and the tenant has

been granted an opportunity to contest any adverse findings through the grievance hearing or other legal procedures.

Applicability

The procedures in this document apply to all THA staff that access EIV data.

Purpose

The purpose of this document is to set forth THA policies and procedures governing the use of the EIV system and associated documents. The practices, controls and safeguards described in this document have been established to ensure compliance with the Federal laws regarding the protection of this information.

Privacy Act

The data provided via the EIV system will be protected to ensure that it is only used for official purposes and not disclosed in any way that would violate the privacy of the individuals represented in the system data. Privacy of data and data security for computer systems are covered by a variety of Federal laws and regulations. The Privacy Act of 1974 as amended, 5 U.S.C. 552(a) is one such regulation.

The full text of the Privacy Act can be accessed at http://www.usdoj.gov/fois/privstat.htm

Security Officer

The EIV Security Officer is the Assistant Executive Director of the Taunton Housing Authority. The security officer is responsible for ensuring that proper technical, physical, and administrative safeguards are in place and enforced. The duties of the security officer are as follows:

Systematically reviews all User IDs issued to determine if the users still have a valid need to access EIV data and modifies or revokes access rights as appropriate.

Annually review the existing EIV policies and procedures.

Conducts file audits, annually, to assure that a copy of Form HUD-9886 has been signed by each member of the household age 18 years or older and is in the household file.

The security officer is responsible for coordinating and conducting annual security awareness training sessions.

Ensuring that any infractions of security procedures are promptly reported to the Executive Director for investigation and enforcement.

Other Quality Control Review

Supervisors assigned to oversee the staff that completes annual recertifications shall routinely conduct audits on completed transactions. As part of any file audit, supervisors will check for a current HUD-9887 and HUD-9887A.

The security officer will conduct an annual review of tenant files to ensure that HUD-9887 forms are in tenant files. Files will be randomly selected. Sample size will be the same sample size outlined in SEMAP regulations for indicator #3-Adjusted Income.

Security Awareness Training

Security awareness training is a vital aspect of ensuring the security of the EIV system and data. Taunton Housing Authority EIV users and potential users will be made aware of the importance of respecting the privacy of data, following established procedures to maintain privacy and security, and notifying management in the event of a security or privacy violation.

Security Awareness training will be provided to each employee upon granting access to the EIV system. Thereafter, annual security awareness refresher training will be provided to each employee with EIV access.

The security officer will conduct security awareness training in the following manner:

The trainer and the employee will both sign a certification that EIV security training has been provided. Documents shall be stored in the EIV security binder.

At the commencement of the training, each employee will also sign the EIV Rules of Behavior and User Agreement form. A copy shall be provided to the employee and the original shall be stored in the EIV security binder.

The security officer will limit the security awareness training to security awareness and compliance issues only. Instructing staff on how to navigate in the EIV modules and how to run reports or to interpret data is the responsibility of the employee's direct supervisor.

The following describes Built in and additional safeguards:

- Each user is required to have their own User ID and Password
- The User ID identifies the user is authorized to access
- Passwords are encrypted
- The system forces all users to change their passwords every 60 days

- After three unsuccessful attempts to log in, the User ID is locked and the user must contact the HUD System Administrator.

- THA staff will not save EIV data to computer hard drive or any other automated information system.

- THA staff will not leave their computer unattended with EIV data displayed on the screen.

- THA staff will not log in using another user's ID

Access to Workspace

The doors to the Taunton Housing Authority are locked at all times. Employees are only granted access, during work hours, to a workspace that is appropriate based on their employment assignment.

Confidential Resident Files

All EIV data will be printed and saved in the corresponding tenant file. Unless an authorized user is working on a transaction, tenant files are maintained in a file cabinet. Tenant files may not be left unattended.

Hard Copy Security Requirement

Staff handling EIV data is assigned an individual printer and shall not be printed to networking printers.

Disposal of EIV Information

EIV Reports must be disposed of under the following circumstances:

- Tenant is terminated from the program
- EIV report was incorrectly requested

EIV reports must be pulled out of tenant files once assistance to a tenant is terminated. It is the responsibility of the employee handling the case to review the file and pull out all EIV reports from the file prior to being stored. EIV reports must be shredded.

A log of disposed EIV records will be stored in a binder by the employee handling the case.

The EIV Security Officer will review the disposal logs concurrent of the annual audit.

Reporting Improper Disclosures

Recognition, reporting and disciplinary action in response to security violations are crucial to successfully maintaining the security and privacy of the EIV system.

Security Violations may include the following:

- Disclosure of private data
- Attempts to access unauthorized data
- Sharing of User IDs and passwords

Upon discovery of a possible improper disclosure of EIV information or another security violation by a THA employee or any other person, the individual making the observation must immediately report the discovery to the Executive Director.

Sanctions

Actions violating any of these rules will result in immediate termination of User ID and password from the system and may result in further disciplinary action (civil or criminal) as prescribed by the Office of the Inspector General.

- **Unauthorized disclosure** can result in a felony conviction and a fine of up to $5,000 and/or imprisonment up to five (5) years, as well as civil penalties.
- **Unauthorized inspection** of data can result in a misdemeanor penalty of up to $1,000 and/or one (1) year imprisonment, as well as civil penalties.