



# **Housing Authority of the City of El Paso**

## **ENTERPRISE INCOME VERIFICATION (EIV)**

### **SECURITY POLICY**

Rev. October 2011

**EIV Security Policy  
Acknowledgment Form**

By signing this form I acknowledge my receipt of the EIV System Security Policy approved by the Chief Executive Officer, and my responsibility to abide by its contents. I further understand and agree to the following:

- This manual represents a summary of the most important policies relative to the EIV System, but is not intended to be all inclusive of the Housing Authority of the City of El Paso (HACEP) policies or practices. It is not intended to be comprehensive or to address all the possible application of, or exceptions to, the general policies and procedures described.
- The Housing Authority retains the sole right in its business judgment to modify, suspend, interpret or cancel in whole or in part at any time, and with or without notice, any of the published or unpublished EIV System policies or practices.

For specific information, I must refer to HUD PIH Notice 2010 – “Administrative Guidance for Effective and Mandated Use of the Enterprise Income Verification (EIV) system, HUD Handbook 2400.25 Rev 1 dated May 2005 (as applicable) and other HUD and HACEP related reference materials since this policy represents only a brief summary.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Employee Name (print)

\_\_\_\_\_  
Job Title

\_\_\_\_\_  
Date

# Table of Contents

	<b>Page</b>
<b>Introduction</b>	<b>4</b>
<b>Applicability</b>	<b>4</b>
<b>Purpose</b>	<b>5</b>
<b>Privacy Act Considerations</b>	<b>5</b>
<b>Section 1:</b> Safeguarding EIV Data	<b>6-7</b>
<b>Section 2:</b> Security Awareness Training	<b>8</b>
<b>Section 3:</b> Reporting Improper Disclosures	<b>9</b>
<b>Section 4:</b> Legal Action	<b>10</b>

## **Introduction**

The Enterprise Income Verification (EIV) System is intended to provide a single source of income-related data to Public Housing Agencies (PHAs) for use in verifying the income reported by tenants in the various assisted housing programs administered by PHAs across the nation. The Office of Public and Indian Housing (PIH) is responsible for administering and maintaining the EIV system.

The EIV system assists PHAs in the up-front verification of tenant income by comparing the tenant income data obtained from various sources including:

- Tenant-supplied income data captured on Form HUD-50058 and maintained in the Public Housing Information Center (PIC) database;
- Wage information from the State Wage Information Collection Agencies (SWICAs);
- Social Security (SS) and Supplemental Security Income (SSI) from the Social Security Administration (SSA); and
- User Profile information from the PIC database.

As of December 29, 2009, HUD mandated the use of the EIV system in its entirety to verify tenant employment and income information during mandatory reexaminations of family composition and income; and reduce administrative and subsidy payment errors in accordance with 24 CFR 5.236 and administrative guidance issued by HUD.

EIV tenant data must be used to verify a tenant's eligibility for participation in a HUD rental assistance program and to determine the level of assistance the tenant is entitled to receive. Any other use, unless approved by the HUD Headquarters EIV Coordinator or EIV Security Officer, is specifically prohibited and may result in the imposition of civil or criminal penalties on the responsible person or persons. Further, no adverse action can be taken against a tenant until the PHA has independently verified the EIV information and the tenant has been granted an opportunity to contest any adverse findings through the established grievance hearing or other legal procedures.

## **Applicability**

The procedures outlined in this document apply to PHAs administering the Public Housing (PH) and the Housing Choice Voucher Program (HCVP). The security procedures outlined in this document apply to all EIV data, regardless of the media on which they are recorded. Computerized media containing EIV data must be afforded the same levels of protection given to paper documents or any other media with EIV data.

## **Purpose**

This policy provides HACEP staff who have been granted access to EIV with practices, controls and safeguards that must be implemented to insure adequate protection of the confidentiality of the tenant income data and compliance with federal laws regarding the protection of this information. EIV documents and/or actions will be integrated into HACEP's occupancy protocols, which also involve Privacy Act related materials, e.g., third-party income, medical and other documents.

## Privacy Act Considerations

The data in EIV contains personal information on individual tenants which is protected under the Federal Privacy Act. The information in EIV may only be used for limited official purposes, as noted below.

### A. Official Purpose Include:

1. PHAs, in connection with the administration of PIH programs, for verifying the employment and income at the time of interim and annual reexaminations.
2. HUD staff for monitoring and oversight of PHA compliance with HUD program requirements.
3. Independent Auditors hired by the PHA or HUD to perform a financial audit for use in determining the PHA's compliance with HUD program requirements, including verifying income and determining the accuracy of the rent and subsidy calculations.

### Restrictions on disclosure requirements for Independent Auditors:

- (a) May only access EIV income information within family files and only within the offices of the PHA or PHA-hired management agent;
- (b) May not transmit or transport EIV income information in any form;
- (c) May not enter EIV income information on any portable media;
- (d) Must sign non-disclosure oaths that the EIV income information will be used only for the purpose of the audit; and
- (e) May not duplicate EIV income information or re-disclose EIV income information to any user not authorized by Section 435(j)(7) of the Social Security Act to have access to the EIV income data.

### B. Official Purposes Does NOT Include:

Sharing the information with governmental or private entities not involved in the reexamination process specifically used for PIH rental assistance programs.

Disclosing the EIV information to other private or public entities for purposes other than determining eligibility and level of assistance for PIH rental assistance programs is prohibited since these entities are not a party to the computer matching agreements with the HHS and SSA. The fact that these entities may find the EIV beneficial for similar eligibility and determination purposes for other low- income housing programs or public benefits, does not permit these entities to use or view information in the EIV system that is covered by the computer matching agreements.

EIV data will only be provided to the adult family member who disputes EIV information. Privacy of data and data security for computer systems are covered by a variety of federal laws and regulations, government bulletins, and other guiding documents. The Privacy Act of 1974 as amended, 5 U.S.C. 552 (a) is one such regulation and EIV data require careful handling in order to assure PHA compliance with the Privacy Act. (See Appendix A Safeguards Provided by the Privacy Act). The Act also describes the criminal penalties associated with violation of policy supporting the Act. (See Appendix B Criminal Penalties Associated with the Privacy Act).

Authorized staff must assure that a copy of the HUD Form-9886, Authorization for the Release of Information/Privacy Act Notice, has been signed by each member of the household eighteen (18) years of age or older and the family head and spouse, regardless of age, and is in the household file. By signing this form, the tenant authorizes HUD and the PHA to obtain and verify income and unemployment compensation information from various sources including current and former employers, state agencies, and the SSA. HUD is relying on the PHAs to have this authorization on file as required by 24 CFR Part 5.230. Information obtained is protected under the Privacy Act.

## Section 1 - Safeguarding EIV Data

Protective measures will ensure that EIV data is used for official purposes only, and not disclosed in any way that would violate the privacy of the individuals represented in the system data. Designated staff will adhere to the following procedures:

- The designation of the EIV Administrator, Security Coordinator, and individuals, who will serve as backups for these positions, will be at the discretion of the Chief Executive Officer. Appointments may include Director of Budgets, Chief Financial Officer, Chief Operating Officer, Director of Section 8, and Director of Public Housing.
- The EIV Administrator will be responsible for approving user access to authorized staff in the Public Housing Department to all staff (including PHA hired management agents) who have a need to access the EIV system, including, but not necessarily limited to, Regional Supervisors, Asset Managers, Assistant Asset Managers, Compliance Manager, Production and Quality Control Technicians, and Eligibility/Admissions staff.
- The EIV Administrator will be responsible for assigning user access to authorized staff in the HCV Department to include HCV Supervisors, HCV Technicians and the HCV Compliance Unit.
- The EIV Administrator will be responsible for approving user access to designated staff in Multifamily Housing to include Multifamily Asset Manager and Assistant Asset Manager.
- The EIV Security Coordinator will be responsible for maintaining and enforcing security procedures.
- HACEP users and recipients of EIV data will ensure compliance with security policies and procedures outlined in this document. Violations will be immediately reported to the EIV Administrator or designee and may lead to disciplinary action up to and including termination of employment.
- Staff involved in the access or receipt of EIV data will ensure that data is used for official purposes only, and not disclosed in any way that would violate the privacy of the individuals represented in the system data.
- EIV data will be handled in such a manner that it does not become misplaced or made accessible to unauthorized personnel.
- In the event that it is necessary to transport tenant files between HACEP offices, the files will be transported in a locked document carrier labeled "Authorized Personnel Only". Files may not be transported via interoffice mail, but must be *hand carried* by authorized staff. Staff will never take resident files home for any reason.
- Users must not duplicate EIV data.
- EIV computer printouts shall immediately be placed in the tenant file. If EIV data is kept in file cabinets, the cabinets must be maintained in a locked room and identified by the use of posted signs indicating "Authorized Personnel Only".
- The Directors of Public Housing and Section 8 will issue keys and track the inventory of keys available, the number of keys issued, and to whom the keys were issued. (See Appendix E Key Accountability Record).
- All employees who are issued keys to security rooms and/or file cabinets will complete a form

acknowledging the receipt of the key(s). The EIV Security Coordinator will maintain these forms. (See Appendix F Acknowledgment of Receipt of Keys).

- The EIV Administrator will maintain a record of all users upon approval by the Chief Operating Officer or designee. (See Appendix D - Access Authorization Form).
- The EIV Administrator will ensure that all users who access the EIV system have a current User Agreement on file. The administrator will secure and maintain such records. (See Appendix D - HUD Rules of Behavior and User Agreement).
- The EIV Security Coordinator will conduct a quarterly review of all user IDs to determine if there is a valid need for access to EIV data. The EIV Security Coordinator will obtain a list of all users and will meet with the Director of Public Housing and the Director of Section 8 to verify whether those listed continue to require access.
- All records maintained by the EIV Administrator and the EIV Security Coordinator will be labeled "Authorized Personnel Only" and will be maintained in a folder separate from other information and files within a filing cabinet. The designated area will be within a locked room.
- Restricted areas will be cleaned only during regular office hours or in the presence of an employee with authorized access.
- Computer screens displaying EIV data will not be left unattended. Computer screens will not be placed in such a way where unauthorized persons may view information. Users will either log out of the system or lock the computer when not in use.
- Computer printouts will be retrieved from a designated printer, as soon as they are generated and will not be left unattended.
- EIV computer printouts that are erroneously generated will be shredded and recorded in a designated.
- Users will not access data through any computer other than the assigned and designated secure computers of HACEP.
- Unauthorized access or known security breaches will be reported to the EIV Administrator and EIV Security Coordinator. The EIV Security Coordinator will notify the Chief Executive Officer and the Director of Human Resources. The Chief Executive Officer will promptly notify appropriate authorities including the HUD Field Office's Public Housing Director.

## **Section 2 - Security Awareness Training**

As a condition of initial and continued access to the EIV System, PHA staff are required to complete Annual Security Awareness training and EIV system training (initial (complete system training). Thereafter, update (interim system changes) training) is required when offered by HUD Headquarters (HHQ). All EIV training must be completed as directed by HUD. Training requirements also apply to those individuals who will not access the EIV system, but will view or handle printed and/or electronic EIV data. Individuals who will view and/or handle printed EIV information are required to complete only annual Security Awareness training (EIV) system training is optional for these individuals). EIV training provided by third parties does not fulfill the mandatory EIV training requirement.

- The EIV Administrator and Security Coordinator will train employees in EIV System security policies and procedures before granting access to EIV information. Attendance records will be maintained. (See Appendix I Security Awareness Training Attendance Record).
- Users will be provided a copy of the HACEP EIV Security Policies and EIV Procedures Manuals.
- Employees will be advised of the penalties associated with the provisions of the Privacy Act of 1974, Section 552(a), which makes unauthorized disclosure or misuse of tenant wage data a crime punishable by a fine of up to \$5,000. (See Appendix B Criminal Penalties Associated with the Privacy Act).
- Employees will be briefed annually thereafter. The EIV Security Coordinator will maintain attendance records. (See Appendix I Security Awareness Training Attendance Record).
- The EIV Administrator and/or the EIV Security Coordinator may communicate security information and requirements to appropriate personnel through various methods outside of the formal trainings and awareness sessions. Methods may include discussions at meetings or security bulletins posted throughout work areas.
- Upon completion of trainings, the EIV Administrator and EIV Security Coordinator will ensure that employees have completed the User Agreement indicating that they are aware of the safeguards and responsibilities associated with using the system. (See Appendix D HUD Rules of Behavior and User Agreement).

### **Section 3 - Reporting Improper Disclosures**

Recognition, reporting, and disciplinary action in response to security violations are crucial to successfully maintain the security and privacy of the EIV system. Security violations may include the disclosure of private data as well as attempts to access unauthorized data and the sharing of User IDs and Passwords.

- Employees making the observation or receiving information with regard to improper disclosure of EIV information or other security violations should contact the EIV Security Coordinator.
- The EIV Security Coordinator will immediately contact the EIV Administrator for the purpose of immediately revoking access to the EIV system until which time a determination is made.
- The Chief Executive Officer should provide the HUD Field Office Public Housing Director with the written documentation.
- The HUD Field Office Public Housing Director upon receipt of the written documentation will make a determination regarding the referral and the provision of the written documentation to the Headquarters EIV Coordinator and/or EIV Security Officer for further review and follow-up action.

#### **Section 4 Legal Action**

In the event of current or pending litigation, legal counsel will provide guidance with regard to applicable documents. If litigation is pending, all applicable documents and records, regardless of disposal date, will be retained until resolution of the legal matter.