

# EIV Policy & Procedure<sup>1</sup>

The Income Reports in **EIV** contain the SSNs, full days of birth, first and last names, and physical address of tenant families. This is all very personal information that **must not** be handled carelessly. Therefore, --*Property Name or Management Company Name*-- realizes that it must be careful not to share this information with anyone who is not authorize3d to have it.

Privacy Act of 1974 ...552a (a) Definitions for purposes of this section— (1) the term “agency” means agency as defined in section 552(f) of this title; (2) the term “individual” means citizen of the United States or an alien lawfully admitted for residence; (3) the term “maintain” includes maintain, collect, use or disseminate; (4) the term “record” means any item, collection or grouping of information.

## **EIV Data** may only be disclosed to:

- Private Owners
- Management Agents
- Service Bureaus
- Contract Administrators
- HUD Staff
- HUD Office of Inspector General (OIG) for investigative purposes
- Individual to whom the record pertains

## **EIV Unauthorized Disclosure**

- Must not disclose data in any way that would violate the privacy of the individuals
- EIV Date must not be disclosed (or re-disclosed) to any third parties

## **Sanctions**

- Willful disclosure or inspection of EIV Data can result in civil and criminal penalties

---

<sup>1</sup> Document developed and distributed by permission from Candi Atkins; Candi Atkins Consulting; 6420 E. Tropicana Ave., Suite #312, Las Vegas, NV 89122; (702) 434-3933; (702) 434-3977 Las Vegas fax; [www.candiatkinsconsulting.com](http://www.candiatkinsconsulting.com)

Unauthorized disclosure – felony conviction and fine up to \$5000.00 and/or imprisonment up to five (5) years, as well as civil damages

Unauthorized inspection – misdemeanor penalty of up to \$1000.00 and/or imprisonment, as well as civil damages

Before accessing the **EIV System**, all employee users must acknowledge, each time that they sign on, that they understand:

- The conditions of the of the Privacy Act
- They may have access to EIV for official purposes only
- They are subject to civil and/or criminal penalties under the Privacy Act of misuse of information
- There must be a signed consent form (HUD 9887 & 9887A) on file before viewing income data from the individual (every family member 18 or older, whether they have income or not must sign these forms)
- The signed HUD 9887 & 9887A must not be older than 15 months

## **Tenant's Right to Dispute EIV Data**

- You must permit individual to have access to information pertaining to them and to request information be amended
- You must independently verify disputed information
  1. Tenant must be notified of findings
  2. Management cannot suspend, terminate, reduce or make a final denial of assistance or tenancy until tenant has opportunity to dispute and discuss

## **EIV Coordinator and User Authorization**

When signing the CAAF (Coordinator Access Authorization Form) or the UAAF (User Access Authorization Form), EIV users agree to:

1. The Rules of Behavior

Delineates responsibilities of, and expectations for, individuals with access to the EIV system, which hold users accountable for their actions and responsibilities

Enhances other HUD policies already in place

Outlines application rules

## Safeguard Categories

- Technical

1. Must have a valid WASS User ID and password

*IDs and Passwords must not be shared;*

*Must not access system using another's ID!!!!*

2. Must provide Management with application access authorization form

*Access to data is restricted based on **EIV** role (Coordinator or User);*

*Access limited based on need to know*

3. Access and activity will be monitored and audited by Management

***EIV** Coordinators must be certified annually;*

***EIV** Users must be certified quarterly (if not certified within 30 days after the end of the current quarter, access to **EIV** is terminated)*

- **Administrative Safeguards**

1. These are the standard operating procedures for use of data from **EIV**

*Use employment and income data for processing HUD 50059s only;*

***Do Not** share data with others who do not have a "need to know";*

*Check to see if the applicant/tenant is receiving assistance under another program at a different location;*

*Owner approval letters must be on file for each "Coordinator" or "User" and be current;*

*Periodically (quarterly) review the list of "Users" at each site to see if "User" still has a valid need to access the **EIV** data for that site or project;*

*Modify or revoke rights as appropriate;*

2. Assign Access to ensure that access rights and responsibilities are appropriate
3. Tenant Consent Form on file
4. Destroy EIV information that is no longer needed in accordance with HUD Handbook 4350.3 requirements – shred, burn or pulverize

*Social Security Benefit (SSA) Reports are to be kept for the term of the tenancy plus (3) three years after tenancy is terminated;*

*NDNH Reports (National Directory of New Hires) from EIV (either electronic or paper) may only be retained for 2 years. Then the information must be destroyed if it contains new hire, wage or unemployment compensation benefit data however any tenant provided documentation, or other third party verification of income, received to supplement the NDNH data must be retained in the tenant file for the term of the tenancy plus three (3) years after tenancy terminated.;*

*If SSA & NDNH benefits are combined in a single report, the retention requirements for NDNH data reports apply;*

*Management will make a notation in the tenant file when NDNH data is destroyed. The notation should state that “the NDNH employment and income information obtained from the EIV system was used for verification of the employment source and, if applicable, for determining the tenant’s income from wages and/or unemployment compensation as well as the date the information was destroyed.*

5. Conduct training to ensure that all EIV users receive security training at time of implementation or employment and at least annually thereafter and maintain a record of such training. Communicate security information through the use of posters, security bulletins, discussion groups and distribution of all current EIV information and memos.
6. Detect, deter and report improper disclosures, unauthorized access or security breaches to Supervisor and/or Management.

## **Physical Safeguards**

1. Designate secure areas by restricting the use of printers, copiers, facsimile machines and maintain controlled access to the areas where they are kept.
2. Secure computer systems and output by storing downloaded **EIV** data in a separate, restricted directory, label CDs containing **EIV** data “confidential: or “For official use only”.
3. Lock in a secure place.
4. Make sure that the computer screen is not visible by any unauthorized persons.
5. Do not use a computer in the reception area for **EIV** reports. If you have to do this, reposition your desk or computer to keep the material confidential.
6. Retrieve all computer printouts as soon as they are generated, so that **EIV** data is not left unattended.
7. Printouts should not be removed from the premises to prevent any identity theft.
8. Avoid leaving a computer unattended with **EIV** data displayed on the screen. Lock your computer/Log off/Exit the system when you are leaving your desk or when finished for the day. **EIV** will time-out after 30 minutes of inactivity.
9. The fastest and safest way to log out or “close” **EIV** and WASS is to click on the “X” in the upper right corner of the screen while in **EIV**.

I, \_\_\_\_\_ agree to follow the above policy and procedures of \_\_\_\_\_ Property Name or Management Company in the use and access to the **EIV System**.

\_\_\_\_\_  
Employee’s Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Supervisor/Owner’s Signature

\_\_\_\_\_  
Date