

Sample EIV – Enterprise Income Verification System Security Policy

Property

INTRODUCTION	2
SECURITY AWARENESS TRAINING.....	3
PHYSICAL SECURITY REQUIREMENTS.....	4
LIMITING ACCESS TO EIV DATA.....	5
EIV SYSTEM COORDINATORS	5
EIV USERS	5
COMPUTER SYSTEM SECURITY REQUIREMENTS	6
USER NAMES, PASSWORDS AND PASSWORD CHANGES.....	7
DISCLOSURE OF EIV INFORMATION	7
USE AND HANDLING OF EIV DATA	8
EIV PRINTOUTS	8
PROVIDING EIV PRINTOUTS TO AUDITORS.....	8
PROVIDING EIV PRINTOUTS TO RESIDENTS.....	9
ELECTRONIC INFORMATION FROM EIV	9
DISPOSAL OF EIV INFORMATION	9
REPORTING IMPROPER DISCLOSURES	9
ACKNOWLEDGEMENT.....	10

INTRODUCTION

The purpose of this policy is to provide instruction and information to staff, auditors, consultants, contractors and applicants and residents for the acceptable use, disposition and storage of data obtained through EIV (Enterprise Income Verification System).

The EIV coordinator for the owner/agent will have the responsibility of ensuring compliance with the security policies and procedures outlined in this document. These responsibilities include:

- Maintaining and enforcing the security procedures
- Keeping records and monitoring security issues
- Communicating security information and requirements to appropriate personnel including coordinating and/or conducting security awareness training sessions
- Conducting review of all User ID's issued to determine if the users still have a valid need to access EIV data and taking necessary steps to ensure that access rights are revoked or modified as appropriate
- Reporting any evidence of unauthorized access or known security breaches to the EIV coordinator for the owner/agent and taking immediate action to address the impact of the breach including but not limited to prompt notification to The EIV coordinator for the owner/agent. to the EIV coordinator for the owner/agent will escalate the incident by reporting to appropriate parties including the Contract Administrator and/or HUD.

The EIV Database is part of HUD's Secure Systems Database. Individual Users must use their own user name (MID/WASS ID) and password to access the Secure Systems database. Coordinators, who are not property owners, have obtained a letter of authorization from the property owner for access to EIV. This letter is maintained in the property's EIV file and will be available to Reviewers during the Management and Occupancy Review.

This policy has been developed to ensure that EIV data is secure. This policy has been communicated to all persons with access to EIV or EIV data. This policy has been developed to ensure compliance with HUD's security protocol regarding the three safeguard categories:

1. Technical
2. Administrative
3. Physical

In order to comply with **Technical Safeguards**:

- Each coordinator/user must have a valid WASS User ID and password
- IDs and passwords **must not be shared**
- No one may access the system using another users identity
- Each user must provide an application access authorization form (CAAF or UAAF)
- Access to data is restricted based on EIV role (EIV Coordinator or EIV User)
- Access is limited based on need to know
- Users understand that access and activity are monitored and audited

To comply with **Administrative Safeguards:**

- The owner/agent has established standard operating procedures for use of data
- Employment and income data is used for certification and compliance purposes only
- Users may not share data with others who do not have a need to know
- Users will check to see if applicant/tenant is receiving assistance under another program at a different location
- The EIV coordinator for the owner/agent will monitor access
 - Obtain and retain owner approval letters
 - Approved/current signed access authorization form
 - Conduct periodic reviews to see if user still has a valid need to access the EIV data
 - Modify or revoke rights as appropriate
 - Assign Access Ensure access rights and responsibilities are appropriate
- Ensure that a signed copy of form HUD-9887 is on file for all adults living in the unit
- Destroy EIV information when it is no longer needed
- Ensure all EIV users receive security training at time of implementation and at least annually thereafter
- Communicate security information
 - Posters
 - Security bulletins
 - Discussion groups
 - Distribution of EIV manuals
- Detect, deter, and report improper disclosures, unauthorized access, or security breaches to the EIV coordinator for the owner/agent who will report as necessary to:
 - HUD's Multifamily Help Desk
 - HUD's Security Officer
 - TRACS/EIV mailbox: MFTRACSSecurity@hud.gov
 - Mail to: Department of Housing and Urban Development Office of Multifamily Housing
 - Notify the Office of Inspector General (IG)
E-mail it to Hotline@hudoig.gov.

The owner/agent has also implemented the following processes to ensure compliance with HUD's

Physical Safeguard requirements:

- Designated secure areas
- Restricted use of printers, copiers, facsimile machines, etc.
- Controlled access to areas containing EIV information
- How to secure computer systems and output
 - If any EIV data is converted to an electronic format, it must be encrypted
 - All emails including EIV data must be encrypted
 - Store downloaded EIV data in a separate, restricted access directory
 - Label CDs containing EIV data "confidential" or "For Official Use Only"
 - Lock in secure place
- Users must retrieve all computer printouts as soon as they are generated so that EIV data is not left unattended
 - Keep printouts locked up
 - Printouts should not be transported from premises
 - Avoid leaving a computer unattended with EIV data displayed on screen
 - Lock computer/Log off/Exit the system when not going to be at desk or when finished for the day (EIV will time-out after 30 minutes of inactivity)
 - Use a password-protected screensaver

- Secure disposal of EIV information
 - Destroy as soon as it has served its purpose or as prescribed by HUD's policies and procedures
 - Burn/shred
 - Keep log of destroyed data
 - Date destroyed
 - How destroyed
 - By whom

SECURITY AWARENESS TRAINING

Security awareness training is a crucial aspect of ensuring the security of the EIV System and data. 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. Before granting access to the EIV information, each person must be trained in EIV Security policies and procedures.

Additionally, all employees having access to EIV Data will be briefed at least annually on the security policy and procedures that require their awareness and compliance. Information about user access and training will be maintained in the property EIV file. See Sample EIV File Checklist.

EIV Users and Coordinators must complete the appropriate EIV Security Awareness Training Questionnaire www.hud.gov/offices/hsg/mfh/rhiip/eiv/securityawareness.pdf before requesting access. Do not send the completed questionnaire to HUD. This must be retained and made available to the reviewer at the Management and Occupancy Review.

After initial setup, **coordinators** must certify **annually**. This is done electronically, through EIV. Copies of the paper CAAF and the most recent, electronic CAAF must be available for review during the Management & Occupancy Review.

After initial setup, **users** must certify **semi-annually**. This is done electronically, through EIV. Copies of the paper UAAF and the most recent, electronic UAAF must be available for review during the Management & Occupancy Review.

PHYSICAL SECURITY REQUIREMENTS

Restricted Areas: The Owner/agent, along with site staff authorized to view EIV data will maintain EIV files in a clearly identified designated management office in a locked file cabinet, when not in active use. The management office is separated from non-restricted areas and will be locked when not in immediate use.

Since the EIV data in resident files is maintained in the locked file room, management will establish and maintain a key control log to track the inventory of keys available, the number of keys issued and to whom the keys are issued. All employees and contractors who have been issued keys to the file room will complete a form acknowledging the receipt of the key. **See EIV Privacy Policy.**

Users will retrieve computer printouts as soon as they are generated so that EIV data is not left unattended in printers or fax machines where unauthorized users may access them. EIV data will be handled in such a manner that it does not become misplaced or available to unauthorized personnel.

LIMITING ACCESS TO EIV DATA

User accounts for the EIV system will be provided on a need-to-know basis, with appropriate approval and authorization.

EIV SYSTEM COORDINATORS

Before accessing EIV, the Secure Systems Coordinators will obtain a letter/memo from each property owner indicating that the owner gives permission for the Secure Systems Coordinator to act as the EIV coordinator. Once that permission is obtained, the Coordinator will

- Review the EIV training material provided by HUD
- Participate in EIV Security Training from HUD or another source
- Read and sign the EIV Security Policy
- Read the EIV Use Policy

Upon completion of these tasks, the EIV Coordinator will submit to HUD, the appropriate Coordinator Access Authorization Forms. Upon receipt of HUD approval, the EIV Coordinator will complete the EIV Coordinator setup process.

EIV USERS

Before requesting EIV User access, appropriate staff will:

- Review the EIV training material provided by HUD
- Participate in EIV Security Training from HUD or another source
- Read and sign the EIV Security Policy
- Read the EIV Use Policy

Upon completion of these tasks, the EIV User will submit, to the EIV Coordinator, the appropriate User Access Authorization Form. Upon receipt, the EIV Coordinator will review the completed Security Awareness Training Questionnaire for accuracy and recommend further training if necessary.

If the EIV Coordinator feels that the EIV User candidate does not understand the security requirements, the EIV Coordinator will not continue with the EIV setup for that user. Under no circumstances will the EIV Coordinator process the User Access Authorization Form unless the signed EIV Security Policy is attached.

Once the tasks are satisfactorily completed, the EIV Coordinator will complete the appropriate steps to provide EIV access to the user. In accordance with HUD requirements, the user's need for access will be reviewed on a semiannual basis.

At least once a year, staff with EIV access will be required to:

- Participate in training that includes a review of the EIV security requirements and
- Complete the EIV Security Awareness Training Questionnaire

The EIV coordinator for the owner/agent will restrict access to EIV data only to persons whose duties or responsibilities require access. EIV Coordinators will be required to request re-certification on an annual basis. EIV Coordinators are authorized to provide access only to those individuals directly involved in the resident certification process and/or compliance monitoring.

EIV Coordinators will carefully review initial and quarterly requests for access and certify only those users who will need access within the next 6 months.

In some cases, EIV information may be provided to auditors charged with ensuring the owner/agent's compliance with HUD requirements. In these cases, the auditor will be required to review and sign the property's Privacy Policy for Auditors and will be required to sign the HUD Rules of Behavior document. These documents will be maintained in the property's EIV File. In addition, the auditor's access will be noted on the EIV File checklist for review during the Management & Occupancy Review.

The EIV coordinator for the owner/agent will maintain a record of users who have approved access to EIV data. Further, the EIV coordinator for the owner/agent will revoke (Terminate) the access rights of those users who no longer require such access.

HUD 9887/9887-A

The HUD 9887 Fact Sheet will be provided to all adult household members required to sign the form. By signing this HUD Form 9887 and HUD Form 9887-A, the applicant/resident authorizes HUD and/or the owner/agent to obtain and verify income and unemployment compensation information from various sources including, but not limited to, the IRS, the Department of Health and Human Services and the Social Security Administration and state agencies.

The EIV coordinator for the owner/agent will assure that a copy of Form 9887 and Form 9887-A has been signed by each member of the household age 18 years or older. The 9887 will be presented at the final eligibility determination, at move-in and/or initial certification and at each annual certification. If a household member turns 18 in the middle of a certification cycle, that household member will be required to sign Form 9887 and Form 9887-A within 30 days of turning 18. (See HUD 9887 Fact Sheet for exceptions due to extenuating circumstances) All HUD-9887's will be placed in a resident file and will be updated on at least an annual basis for each adult household member.

COMPUTER SYSTEM SECURITY REQUIREMENTS

All computer systems and computers will have password restricted access. Passwords must be no fewer than 8 characters and must include:

- At least one lower case letter
- At least one upper case letter
- At least one number or character such as a dash or exclamation point

The owner/agent will also use Antivirus software to limit data destruction or unintended transmission via virus, worms, Trojan horses or other malicious means. Remote access by other computers other than those specifically authorized is prohibited.

Authorized users of EIV data are directed to avoid leaving EIV data displayed on their computer screens where unauthorized users may view it. A computer will not be left unattended while the user is "logged in" to Secure Systems. If an authorized user is viewing EIV data and an unauthorized user approaches the work area, the authorized user will lessen the chance of inadvertent disclosure of EIV data by logging out of Secure Systems or minimizing or closing out the screen on which the EIV data is being displayed.

USER NAMES, PASSWORDS AND PASSWORD CHANGES

Many systems require frequent changes to passwords. Secure Systems / EIV passwords will be changed in accordance with HUD Secure Systems requirements. Users will not share passwords with any other employee or with anyone outside the organization. EIV access granted to an employee or authorized user will be revoked when access is no longer required or prior to termination of that employee or user to ensure data safety.

Termination of EIV access and un-assigning property access through “Property Assignment Maintenance” is required.

The EIV file will be documented to indicate when user access was terminated by the EIV Coordinator. Documentation of termination will be maintained in the property EIV file.

DISCLOSURE OF EIV INFORMATION

The EIV Social Security (SS), Supplemental Security Income (SSI), new hires (W-4), wage, and unemployment compensation information contained in the EIV system may only be used for limited official purposes.

- By Contract Administrators (CAs) for monitoring and oversight of the resident recertification process
- By the Office of the Inspector General (OIG) for investigative purposes.
- By owners/agents (O/As) for verifying the employment and income at the time of certification for residents **participating in one of HUD’s rental assistance programs listed:**

EIV Data may be disclosed to:

- Private owners
- Management agents
- Service Bureaus
- Contract Administrators
- HUD staff
- HUD Office of Inspector General (OIG) for investigative purposes
- Independent public auditors (IPAs) auditing an owner’s compliance with HUD’s verifying income and the accuracy of rent/subsidy determinations
- Individual to whom the record pertains

EIV income data may only be used for verification of employment and income at certification. Under no circumstances may users or coordinators provide access to the system by sharing the user name/password combination. Owner/agents must not disclose data in any way that would violate the privacy of the individuals.

EIV data must not be disclosed (or re-disclosed) to any third parties such as the local Welfare office, DFCS, etc. Willful disclosure or inspection of EIV data can result in civil and criminal penalties.

- Unauthorized disclosure – felony conviction and fine up to \$5,000 or imprisonment up to five (5) years, as well as civil damages
- Unauthorized inspection – misdemeanor penalty of up to \$1,000 and/or one (1) year imprisonment, as well as civil damages

Official use **does not include** using the EIV data for certifying residents under the Low Income Housing Tax Credit (LIHTC) or Rural Housing Services (RHS) Section 515 programs. Neither the Internal Revenue Service (IRS) nor RHS are a party to the computer matching agreements HUD has with the Department of Health and Human Services (HHS) and with the Social Security Administration (SSA).

The fact that there is financing through other federal agencies involved in a particular property under one of the authorized HUD programs **does not** permit that federal agency to **use or view** information from the EIV system for certifying residents for their programs or for monitoring purposes. Additional third party Income verification will be obtained from the source for use for Tax Credit or Rural Housing Service programs. For Social Security and Medicare information, the resident file will include a current SSA Benefit/Award letter or some other acceptable verification documentation. For employment income and unemployment income, the resident file will contain verification documents as provided in HUD Handbook 4350.3 Revision 1, Appendix 3.

USE AND HANDLING OF EIV DATA

EIV Data serves two purposes:

1. Verification of specific income information provided by the resident
2. Monitoring resident and staff compliance

Use of the data is described in the EIV User Policies. This policy is designed to describe the security protocol used to protect EIV data.

EIV Data will be used only to administer HUD programs. The data in EIV is not to be used to assist with eligibility determination or compliance monitoring for any other programs including those administered by the IRS (Tax Credit) or Rural Development (515).

EIV PRINTOUTS

In addition to use by the owner/agent, EIV reports may also be used by Contract Administrators (CAs) (Performance Based Contract Administrators (PBCAs), Traditional Contract Administrators (TCAs) and HUD staff) for monitoring compliance with the recertification process; independent public auditors (IPAs) auditing an owner's compliance with HUD's verifying income and the accuracy of rent/subsidy determinations; and, the Office of Inspector General (IG) for auditing purposes.

EIV Income Reports are retained in the resident file for the term of tenancy and for three years after tenancy ends. If this property also participates in other housing assistance programs (LIHC or 515) the owner/agent will take special precautions to ensure the security of the EIV printouts. EIV printouts will be maintained in the resident file but will be kept in a separate section of the file and will be removed if the file is to be audited or reviewed by any authorized party for purposes other than those defined by HUD. An alternative would be to keep the EIV printouts in a separate secure location within the management office. EIV printouts will be provided to approved parties, when required, to facilitate compliance with HUD requirements and the property's EIV Use Policy.

PROVIDING EIV PRINTOUTS TO AUDITORS

Independent auditors (IPAs) are approved to view EIV information, when hired by an owner to perform the financial audit of the project, for use in determining the owner's compliance with verifying income and determining the accuracy of the rent and subsidy calculations.

Restrictions on disclosure requirements for IPAs:

- (a) Can only access EIV income information within hard copy files and only within the offices of the owner or management agent;
- (b) Cannot transmit or transport EIV income information in any form;
- (c) Cannot enter EIV income information on any portable media;
- (d) Must sign non-disclosure oaths (Rules of Behavior) that the EIV income information will be used only for the purpose of the audit; and
- (e) Cannot 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.

PROVIDING EIV PRINTOUTS TO RESIDENTS

If a resident requests a copy of their own EIV printout, a copy will be produced. The staff person providing the copy will note that the printout is a copy provided to the resident upon request. This note will include the following:

- **This is not an original, this is a copy provided to: Resident Name**
- **On _____, 20__**
- **By _____ (name will be printed)**
- **Resident Initials _____**

The appropriate staff will make a note in the file any time a copy of the EIV data is obtained by authorized persons. This includes copies provided to the applicant/resident, staff responsible for compliance monitoring, other internal staff, HUD, CA or OIG staff. Under no circumstances will the EIV information be provided to anyone other than those noted in this Security Policy.

ELECTRONIC INFORMATION FROM EIV

In some cases, there may be a need to send or store EIV information electronically. If EIV data is converted to an electronic format, the information will be stored in a special, restricted password protected directory and encrypted using an NIST compliant vendor. All emails that contain EIV data will be encrypted as well. No data will be converted or transported by portable media. EIV data converted to an electronic format will be destroyed in accordance with HUD's recordkeeping requirements and HUD's data share agreement with HHS and SSA.

DISPOSAL OF EIV INFORMATION

EIV data will be destroyed in a timely manner based on the information provided in HUD's published EIV training materials, HUD notices or as prescribed by the owner/agent's policy and procedures. The owner/agent's policy and procedures will not allow data retention that is longer than the time allowed in the published HUD materials. Information about use of EIV information and how printouts were destroyed will be maintained in the EIV file.

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. These security violations may include the disclosure of private data as well as attempts to access unauthorized data and sharing of passwords.

Upon the discovery of a possible improper disclosure of EIV information or other security violation by an employee or any other person, the individual making the observation or receiving the information will contact the EIV Coordinator, who will document all improper disclosures in writing providing details including who was involved, what was disclosed, how the disclosure occurred, and where and when it occurred. The EIV Coordinator will immediately review the report of improper disclosure and, if appropriate, the EIV Coordinator will remove EIV access.

Improper disclosure of any information could be grounds for immediate termination. All employees must carefully review the EIV Access Authorization Form or the Rules of Behavior to understand the penalties for improper disclosure of EIV data.

ACKNOWLEDGEMENT

By signing this form, I acknowledge that I have read and understand the EIV Security Requirements. I agree to abide by this policy and to report any improper disclosure of information.

Name (please print)

Signature

_____/_____/_____
Date

CC: Personnel File
Property EIV File