(EIV) ENTERPRISE INCOME VERIFICATION SYSTEM SECURITY POLICY

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

The purpose of EIV is to assist the HUD, Contract Administrators, owners and their agents in streamlining the income verification process and to help in minimizing the need for 3rd party verification. EIV allows the user to identify:

- Applicants currently receiving HUD assistance
- Income not previously reported
- New employment
- Historical patterns of earnings and received income
- Multi-subsidy for household members included in both PIC and TRACS databases
- Deceased household member(s)

The data provided via 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, government bulletins, and other guiding documents.

Confidentiality:

All information in the applicant/resident file is **personal and private.** The information is strictly confidential and not to be given out to anyone without written authorization.

Applicants/residents are ***not*** allowed to have copies of the EIV data for other adult household members without a signed release from the person(s) involved.

Safeguarding EIV Data

The information processed by any EIV system can include wage and income data about private individuals, as well as identifying information such as Social Security Number, Address, and Employment information. This policy describes methods to comply with HUD's required EIV safeguards.

Technical Safeguards:

1. Reduce the risk of a security violation related to the EIV system's software, network, or applications.
2. Identify and authenticate all users seeking to use the EIV system data.
3. Deter and detect attempts to access the system without authorization.
4. Monitor the user activity on the EIV system.

Administrative Safeguards:

The EIV Coordinator(s) will:

1. Ensure that access rights, roles, and responsibilities are appropriately and adequately assigned.
2. Train staff on security measures and awareness, preventing the unauthorized accessibility and use of data.

The Owner/Agent will:

1. Protect copies of sensitive data and destroy system-related records to prevent reconstruction of the contents.
2. Ensure authorized release of tenant information consent forms (9887 &9887A) are included in all resident files, before accessing and using data.
3. Maintain, communicate, and enforce standard operating procedures related to securing EIV data.

Physical safeguards

The Owner/Agent will:

1. Establish barriers between unauthorized persons and documents or computer media containing private data.
2. Clearly identify restricted areas by use of prominently posted signs or other indicators.
3. Develop a list of authorized users who can access restricted areas-e.g., contractors, maintenance, and janitorial/cleaning staff.
4. Prevent undetected entry into protected areas and/or documents.
5. Notify Coordinators/Security Administrators of system breaches and penetration by unauthorized users.
6. Maintain and enforce the security procedures
7. Keep records and monitor security issues
8. Report any evidence of unauthorized access or known security breaches to the company **EIV Coordinator.**

The EIV Coordinator will:

1. Communicate security information and requirements to appropriate personnel including coordinating and conducting security awareness training sessions.
2. Conduct review of all use ID’s issued to determine if 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.
3. In case of a breach will escalate the incident by reporting to appropriate parties including the Contract Administrator or HUD.

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.

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's EIV file.

EIV System Coordinators

Before accessing EIV, the Secure Systems Coordinator(s) will obtain a letter 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 and complete the appropriate Security Awareness Training Questionnaire and review the EIV Security Policy and the EIV User Policy. Upon completion of these three 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. He/She will then complete the appropriate Security Awareness Training Questionnaire and then review the EIV Security Policy and the EIV User Policy. Upon completion of these three 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.

Note: Under no circumstances will the EIV Coordinator process the User Access Authorization Form unless the executed Security Awareness Training Questionnaire, the signed EIV Security Policy and the signed EIV User Policy are attached.

Once the user request information is 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 quarterly 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 policy and
- Complete the EIV Security Awareness Training Questionnaire

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 90 days.

The EIV Coordinator will maintain a record of users who have approved access to EIV data. Further, **EIV Coordinator** will revoke (expire) the access rights of those users who no longer require such access or modify the access rights if a change in the user's duties or responsibilities indicates a change in the current level of privilege.

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 move-in and/or initial certification. If a household member turns 18 in the middle of a certification cycle, that household member should sign Form 9887 and Form 9887-A **within 7 days of turning 18**. (See HUD 9887 Fact Sheet for exceptions due to extenuating circumstances) All HUD-9887's will be placed in the resident file and will be updated on an annual basis (during the annual recertification process) for each adult household member.

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, current and former employers and state agencies.

User Names, Passwords and Password Changes

Many systems require frequent changes in passwords. Secure Systems/ EIV passwords will be changed in accordance with HUD Secure Systems requirements. Users will ***not*** share user names or 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 Management Office in the employee's personnel file and in the property's EIV file.

Computer System Security Requirements

All computer systems and computers will have password restricted access. The Owner/Agent will also use Antivirus software to limit data destruction or unintended transmission via virus, worms, 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 minimizing or closing out the screen on which the EIV data is being displayed.

Physical Security Requirements

The EIV data may be maintained **in a locked metal file cabinet.**

Since the EIV data in resident files is maintained in the locked file cabinet that may also be in a locked room, **designated staff** 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.

Users will retrieve computer reports 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.

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 Reports/Data

Reports available through EIV will not be printed to a shared printer unless the EIV user plans to immediately retrieve the data. It is preferred that all EIV reports are sent to the user's personal printer. EIV reports will be stored in the resident file. This entire file will be made available to authorized people including appropriate staff or contractors (i.e. Service Bureaus, contractors performing file reviews, etc.) for the Owner/Agent, HUD staff, Contract Administration staff and the Office of the Inspector General.

EXCEPTION regarding properties with Housing Tax Credit or 515 Section 8 "layering": Neither the EIV report(s) nor the Documentation of EIV Data will be provided to any Tax Credit nor 515 Auditor since EIV may not be used to verify information for residents participating in those programs. Alternative verification documents must be used to verify income for Housing Tax Credits or 515 Section 8 programs. For Social Security and Medicare information, employment income and unemployment income, the resident file should contain verification documents as provided in HUD Handbook 4350.3, REV-1, Change 3, Appendix 3.

Further the EIV reports that are required by HUD must be kept in a separate legal sized manila envelope in each resident file for Housing Tax Credit and/or 515 Section 8 layered properties. During Management

Reviews by auditors for Housing Tax Credit or 515 Section 8, the manila envelope containing EIV information must be removed, stored securely and returned to the resident file at the end of the Review.

If other people are tasked with reviewing the file, such as financial auditors complying with the Consolidated Audit Guide (Handbook IG 2000.04), the EIV reports included in the manila envelope will be removed from the file. However, EIV "data" such as Social Security and Employment Income information, etc. will remain in the file to provide appropriate "proof of income" information required by the file audit.

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

- This is not an original, this is a photocopy provided to:_____
- On _____ ____, 20__
- By_____(name will be printed)
- Initials_____

The appropriate staff will place this information the resident file any time a copy of the EIV data is obtained by authorized persons and taken off site. This includes copies provided to the applicant/resident, other internal staff, HUD, Contract Administrator or OIG staff. Under no circumstances will the EIV information be provided to anyone other than those noted in this paragraph.

Other Requirements

Since not all site staff will have access to the EIV database, a designated Management staff person will be responsible for providing income verification and discrepancy information to the site. Information must be sent in such a way as to ensure the security of the data. Preferably, if needed, information will be sent electronically via email or via electronic fax. The email will be opened by the appropriate site staff person, the information will be printed and the email will be immediately deleted from the recipient's email box.

If necessary, reports/data will be produced by designated Management staff and sent express mail. In this case the recipient will be required to sign for the package to ensure that the information is delivered and there is no risk of disclosure to unauthorized persons.

Immediately upon receipt, the reports/data will be filed and secured as appropriate.

Electronic Information from EIV

Under no circumstances should anyone save or scan EIV information to retain an electronic copy. In order to ensure compliance with HUD's security requirements, EIV information should only be produced in hard copy and maintained in accordance with the recordkeeping requirements outlined by HUD.

Alternative

In some cases, there may be a need to send or store EIV information electronically. If there is need to store the information on a hard drive, a specific folder will be created. The folder will be password protected to prevent unauthorized access. Information in the folder will be purged periodically to comply with HUD's EIV file retention policies.

If EIV information is copied to portable media (CD, DVD, tape, etc.) that portable media will be destroyed appropriately upon completion of the intended use.

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 User ID's and 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 and **designated staff member** 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 is grounds for immediate termination. All employees should carefully review the EIV Access Authorization Form to understand the penalties for improper disclosure of EIV data.

Disposal of EIV Information

EIV data used as third party verification will be kept for the term of tenancy plus three years after tenancy is terminated per HUD EIV requirements. Once the retention period has expired, the Owner/Agent must *destroy* the data in a manner that will prevent any unauthorized access to personal information: burn, pulverize, shred, etc.

As necessary, once the EIV originals have been destroyed, information about how EIV reports/data were destroyed will be maintained in the on-site EIV file.