Boyne City Housing Commission
EIV Security and Procedure Policy

Adopted by the BCHC Board of Commissioners 4/23/2025

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 who are 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)

In addition, information in EIV can be used to provide more comprehensive oversight to compliance policies and their implementation. 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.

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.
5. Ids and passwords must not be shared.

Administrative safeguards

1. Ensure that access rights, roles, and responsibilities are appropriately and adequately assigned.
2. Protect copies of sensitive data and destroy system-related records to prevent reconstruction of the contents.
3. Ensure authorized release of tenant information consent forms are included in all family files, before accessing and using data.
4. Maintain, communicate, and enforce standard operating procedures related to securing EIV data.
5. Train staff on security measures and awareness, preventing the unauthorized accessibility and use of data.

Physical Safeguards

1. Establish barriers between unauthorized persons and documents or computer media containing private data.
2. Restrict use of printers, copiers, facsimile machines, etc.
3. Prevent undetected entry into protected documents.
4. Notify Coordinators/Security Administrators of system breaches and penetration by unauthorized users.

The Executive Director/designee 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 including keeping records/monitoring security issues
- Communicating security information and requirements to appropriate personnel including coordinating and conducting security awareness training sessions
- Conducting review of all User IDs 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 and taking immediate action to address the impact of the breach including but not limited to prompt notification to HUD. The Executive Director 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 EIV file.

EIV System Coordinators

Before accessing EIV, the Secure Systems Coordinators will review the EIV training material provided by HUD and complete the appropriate Security Awareness Training Questionnaire and review the EIV Security and Procedure 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 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 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 Security Awareness Training has been completed and the signed EIV Security and Procedure 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

Boyne City Housing Commission (PHA) 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 PHA will maintain a record of users who have approved access to EIV data. Further, PHA will revoke (terminate) 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 PHA will ensure that a copy of Form-9886-A has been signed by each member of the household age 18 years or older. The 9886-A 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 9886-A within the thirty (30) days of the 18th birthday. All HUD-9886-A's will be placed in a resident file and will be updated on an annual basis for each adult household member, as needed. By signing this HUD Form 9886-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.

Usernames, 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 usernames 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 property 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, 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 minimizing or closing out the screen on which the EIV data is being displayed.

Physical Security Requirements

The PHA may use a combination of methods to provide physical security for resident file records. The EIV data may be maintained **in locked metal file cabinets.**

Restricted Areas

Since the EIV data in resident files is maintained in the locked file cabinets, only designated staff will have access to the locked file cabinets. 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.

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 Printouts

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 printouts are sent to the user's personal printer. The Documentation of EIV Data will be included 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. When other people are tasked with reviewing the file, such as financial auditors complying with the Consolidated Audit Guide (Handbook IG 2000.04), EIV Data will remain in the file to provide appropriate information to determine the compliance with verifying income and determining the accuracy of the rent and subsidy calculations.

If a resident requests a copy of their own EIV printout, a copy will be produced. The staff person providing the copy will note in the file that the printout is provided to the resident upon request. This note will include the date and the initials of providing staff. The appropriate staff will make a note in the 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, CA, or OIG staff. Under no circumstances will the EIV information be provided to anyone other than that noted in this paragraph. EIV Income Reports are retained in the resident file for the term of tenancy and for three years after tenancy ends.

Electronic Information from EIV

EIV information may be stored electronically if the system is secured, access is restricted to authorized users, and the storage method complies with HUD EIV security requirements.

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.

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 immediately 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 will be destroyed in a timely manner based on the information provided in HUD's published EIV training materials and HUD notices. The owner/agent's policy and procedures will not allow data retention that is longer than the time allowed in the published HUD materials. As necessary, all EIV originals will be shredded on-site. Information about use of EIV information and how printouts were destroyed will be maintained in the resident file.