



**Office of Public and Indian Housing (PIH)
Enterprise Income Verification (EIV) System
User Access Authorization Form and
Rules of Behavior and User Agreement**

Paperwork Reduction Notice: The information collection requirements contained in this notice have been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995 (44 U.S.C. 3520) and assigned OMB control number(s) 2577-0267. In accordance with the Paperwork Reduction Act, HUD may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the collection displays a currently valid OMB control number.

Public reporting burden for this collection of information is estimated to average 1.0 hour for initial responses and 0.25 hours for modified responses. This includes the time for collecting, reviewing, and reporting the data. The Federal Privacy Act (5 USC 552a) requires that HUD account for all individuals who will have access to a system containing personally identifiable information. The information is being collected to ensure only authorized users have access to HUD's EIV system and that those users are aware of their responsibility to safeguard sensitive data.

Purpose of this form: To request, modify, or terminate access to the PIH EIV system. To review and acknowledge Rules of Behavior and signify compliance with User Agreement.

Send completed forms: To the designated HUD EIV Coordinator at the local HUD office as listed in the instructions. **Note:** Individuals who will not access the EIV system, but will view and/or handle printed or electronic EIV information, are not required to send this completed form to the HUD EIV Coordinator.

PART I. ACCESS AUTHORIZATION

Check here if you will not have access to the EIV system and will only view or handle printed or electronic EIV information

A. Authorized User Details		
1. PHA Code: (e.g. DC451)	2. HUD Office, PHA, or Management Agent Name:	3. Address:
4. Name (first name, middle initial, last name):		5. WASS User ID (C/H/M-ID):
6. Position Title:		7. Phone Number:
8. Email Address:		9. Fax Number:
10. Type of work which involves use of the EIV system or printed and/or electronic EIV information: <input type="checkbox"/> 1 – Initial eligibility only <input type="checkbox"/> 2 – Annual/interim reexams <input type="checkbox"/> 3 – Security Administrator <input type="checkbox"/> 4 – Request EIV access <input type="checkbox"/> 5 – Certify EIV users <input type="checkbox"/> 6 – Modify/terminate EIV access roles <input type="checkbox"/> 7 – HUD Administrator <input type="checkbox"/> 8 – Auditor <input type="checkbox"/> 9 – Investigator/Program Compliance <input type="checkbox"/> 10 – Enter/update/delete debts owed to PHAs & adverse termination information of former tenants <input type="checkbox"/> 11 – Clerical/Administrative Support (Viewer or handler of EIV reports) – Do not complete sections B-E.		

B. Type of Action Requested <i>(See instructions)</i>	
1 – Add Access (Initial access request for new users)	
2 – Reinstatement (Due to automatic system or other termination)	
3 – Modify Access (Add/remove access roles for existing users)	
4 – Terminate Access	

C. PHA User Access Roles – External Users <i>(See instructions)</i>	
<input type="checkbox"/> 1 – PHA Occupancy – Public Housing	<input type="checkbox"/> 5 – Program Administrator – Voucher (Section 8)
<input type="checkbox"/> 2 – PHA Occupancy – Voucher (Section 8)	<input type="checkbox"/> 6 – PHA User Administrator
<input type="checkbox"/> 3 – PHA Occupancy – Applications Processor	<input type="checkbox"/> 7 – PHA Security Administrator
<input type="checkbox"/> 4 – Program Administrator – Public Housing	<input type="checkbox"/> 8 – Other Prescribed by HUD

D. Public Housing Portfolio		
<i>Specify the Public Housing project numbers to which access will be limited.</i>		
<input type="checkbox"/> Check here to grant access to all public housing projects		
Project Number	Project Number	Project Number
1)	4)	7)
2)	5)	8)
3)	6)	9)

E. HUD User Access Roles – Internal Users <i>(See instructions)</i>				
Select Region <i>(Check only one region)</i>	HHQ	HUB	FO	TARC
<input type="checkbox"/> 1 – Occupancy Specialist	<input type="checkbox"/> 5 – HQ PIH DHAP			
<input type="checkbox"/> 2 – Security Administrator	<input type="checkbox"/> 6 – HQ System Administrator			
<input type="checkbox"/> 3 – User Administrator	<input type="checkbox"/> 7 – HQ PIH Help Desk/TAC			
<input type="checkbox"/> 4 – HUD OIG	<input type="checkbox"/> 8 – Other Prescribed by HUD			

F. Authorization

As the Authorizing Official, I authorize the above-named person to have access to the EIV system or view printed or electronic EIV information, as indicated by my signature below. I further understand this form for each user must be maintained on-site by the PHA and may be subject to audit at any time.

Authorizing Official's Name (Print Full Name) Authorizing Official's Signature Date

Check here for **ELECTRONIC SIGNATURE** (Original signed document **must** be on file and is subject to inspection)

G. For HUD Use Only <i>(Maintain a copy of this completed form in your files)</i>	
Date Application Received:	Date Application Processed:
HUD EIV Coordinator's Name:	
Action taken:	Reason:
Approved	
Denied	

PART II. RULES OF BEHAVIOR

A. Introduction

The U.S. Department of Housing and Urban Development (HUD) actively implements policies and procedures to keep its systems secure from unauthorized access and inappropriate use. In compliance with Federal laws and regulations, HUD's Office of Public and Indian Housing (PIH) created these Rules of Behavior for the Enterprise Income Verification (EIV) system to ensure that EIV system users (including those individuals who only view or handle printed or electronic EIV information) comply with HUD's security policies. In addition, this document ensures that system accounts are used in the appropriate manner.

Information contained in the EIV system is for official use only. HUD may grant limited system access to the following classes of individuals: HUD employees, HUD contractors, Public Housing Authority employees, and Public Housing Authority-hired management agents. As a condition of receiving access, all users are required to understand and abide by the HUD's system security policies and procedures.

All users must adhere to the Rules of Behavior outlined in this document. These rules delineate the responsibilities of and expectations for all individuals accessing EIV information. Failure to comply with these rules will result in sanctions. Sanctions may include temporary suspension of system access or permanent termination of all access rights. Additional civil or criminal penalties may result from a misuse of EIV information. (See Part III of this document for more information.)

B. Responsibilities

HUD-PIH, as the System Owner of EIV, is responsible for ensuring that appropriate technical, operational, and managerial security controls are implemented in the EIV system.

Users are responsible for the protection of passwords, information, equipment, systems, networks, and communication pathways to which they have access. All HUD computer resources, including hardware, software, programs, files, paper reports, and data are the sole property of HUD.

C. Other Policies and Procedures

The Rules of Behavior do not replace existing HUD security policies or procedures. These rules are intended to enhance and clarify the specific rules each user must follow while accessing the EIV system. These rules are consistent with the policies and procedures described in the following HUD document:

HUD Information Technology Security Policy. HUD Handbook 2400.25 Rev.-2, CHG-2, dated August 22, 2011, or as amended, establishes responsibilities, practices, and conditions that directly or indirectly promote security in the development, operation, maintenance, and support of all HUD information technology (IT) resources.

This handbook is available online at:

<http://www.hud.gov/offices/adm/hudclips/handbooks/admh/2400.25/index.cfm>. The HUD information security policies are based on recent federal laws, regulations, and guidance on information security (from National Institute of Standards and Technology (NIST)). In areas where federal guidelines are lacking or still evolving, the policy reflects established best security practices within the security community.

D. Application Rules

The Web Access Security System (WASS) user identification (user ID) and password issued to you is to be used solely in connection with the performance of your responsibilities in support of HUD's mission and administration of HUD rental assistance program, and may not be used for personal or private gain. You agree to be responsible for the confidentiality of the assigned information and accountable for all activity with your user ID. Furthermore, you agree that you will not provide this confidential user ID and password to another user during employment nor upon leaving the employment of the agency. Additional rules of the EIV system are as follows:

Required Training – EIV system users are required to participate in annual Security Awareness Training and HUD-sponsored initial and updated PIH-EIV System training. Individuals who will not access the EIV system, but will view and/or handle printed or electronic EIV information are required to participate in only the annual Security Awareness training. Free HUD-sponsored Security Awareness and EIV training is available online at <http://www.hud.gov/webcasts/archives/iv.cfm>. PIH-sponsored EIV training materials are located at <http://www.hud.gov/offices/pih/programs/ph/rhiip/training.cfm>. ***Users are not permitted to access the EIV system or view printed or electronic EIV information if they have not completed the required training.***

System Access (on-site only): Users are required to use only approved HUD software, software settings, and comply with vendor software license agreements. Users are allowed to access the system only using the mechanisms specified by HUD.

Unofficial use of government information: Users must be aware that personal use of information resources is prohibited. EIV data is personal information covered by the Federal Privacy Act (5 USC 552a), as amended, and penalties apply to the misuse of that data. State and local laws may also prohibit misuse of personal information and impose penalties for misuse of the data.

Information protection: Users must avoid leaving system output records or reports unattended or unsecured. Users should lock the computer or log out of the system when leaving work areas unattended. Users shall not violate the Federal Privacy Act (5 USC 552a), as amended, which requires confidentiality of personal data contained in government and contractor data files. Users should securely store EIV data in accordance with HUD policy.

Use of passwords: User passwords and user IDs are for your individual use only and are confidential HUD information. Users are required to change passwords every 30 days. Users are encouraged to avoid creating passwords that can be easily associated with you or your user ID.

System privileges: Users are given access to the system and EIV data based on a need to perform specific work related only to the administration of the following PIH programs: Public Housing, Housing Choice Voucher (HCV), Project-Based Voucher, Project-Based Certificate, and Disaster Housing Assistance programs. Users shall only access the information for which they are authorized.

Individual accountability: Users shall be held accountable for their actions while accessing the system or viewing printed or electronic EIV data. Be aware that all computer resources are monitored and audited.

Monitoring of EIV System Use: All users and agencies are subject to monitoring of their EIV system use and compliance with security requirements by HUD, HUD contractors or a third party. If it is determined that an agency or any of its users are not in compliance with security requirements or any provision of this document, HUD will immediately terminate one or all of an agency's users' EIV access. HUD will reinstate access upon the successful implementation of corrective action(s) to cure the deficiency.

Automatic EIV System Terminations: A user's EIV system access is automatically terminated if the user does not access HUD's Web Access Security Subsystem at least once every 90 days; or if the user is not certified by the respective EIV User Administrator.

Incident Response: Users should immediately contact their supervisor and the HUD Headquarters Security Officer at EIV_help@HUD.GOV, with a copy to local HUD office, regarding any suspected violation or breach of system security.

PART III. USER AGREEMENT

I have read the above policy regarding system security awareness and practices when accessing HUD’s information technology resources. I understand the policies and procedures as set forth above, and I agree to comply with these requirements as a condition of being granted limited access to the EIV system and/or its data.

As an authorized user of the EIV system or viewer and/or handler of EIV data, I understand the information obtained may only be used for official HUD business. I understand that authorized users may access, disclose, inspect and use these data only within the scope of their official duties of administering a HUD rental assistance program. HUD employees are held to the highest level of responsibility and accountability for the protection of HUD data. HUD contractor firms will be expected to apply similar standards to their employees. Anyone who abuses EIV access privileges may be stripped of those and other access rights to HUD’s secure systems. Employees of an agency may be subject to personnel discipline consistent with applicable personnel rules. Contractor firms that do not assure that the Rules of Behavior are observed may be subject to remedies under the terms of their contract.

I also understand that unauthorized disclosure or inspection of EIV data may result in civil and criminal penalties. The penalties are as follows:

- **Unauthorized disclosure** may result in me being found guilty of a misdemeanor and fined not more than \$5,000 and/or imprisoned up to five (5) years.
- **Unauthorized inspection** of EIV data may result in me being found guilty of a misdemeanor and fined not more than \$5,000 and/or imprisoned up to five (5) years.

I understand that my user ID and password are to be used only by me. Under no circumstances will I reveal or allow use of my user ID or password by another person. Nor will I use another person’s password and user ID. I will protect EIV data within my control, whether online, printed, or stored in media, from unauthorized access and disclosure.

I understand and agree to follow all HUD standards, policies, and procedures.

I certify that I have: 1. participated in the initial PIH EIV system training, and 2. within the past twelve (12) months the security awareness training, and 3. I agree to participate in annual security awareness training and 4. periodic PIH-EIV system training as required by HUD.

Failure to provide this certification or participate in training will result in denial or discontinuation of EIV Access.

User’s Name
(Print Full Name)

Date

User’s Signature

Check here for **ELECTRONIC SIGNATURE** (Original signed document **must** be on file and is subject to inspection)

Note: All EIV system users are required to complete initial EIV system training provided by HUD prior to accessing the system. All individuals who will view and/or handle printed or electronic EIV information are required to complete annual Security Awareness training. Security Awareness training provided by third parties is acceptable when HUD has not offered such training.