OMB Approval No. 2506-0171 exp 10/31/2016

IDIS OnLine Access Request

U.S. Department of Housing and Urban Development
Office of Community Planning and Development

Privacy Act Statement: Public Law 97-255, Financial Integrity Act, 31 U.S.C. 3512, authorizes the Department of Housing and Urban Development (HUD) to collect all the information which will be used by HUD to protect disbursement data from fraudulent actions. The purpose of the data is to safeguard the Integrated Disbursement and Information System (IDIS) from unauthorized access. The data are used to ensure that individuals who no longer require access to IDIS have their access capability promptly deleted. This information will not be otherwise disclosed or released outside of HUD, except as permitted or required by law. Failure to provide the information requested on the form may delay the processing of your approval for access to IDIS.

Public Reporting burden for this information collection is estimated to average 30 minutes including time for collecting, reviewing, and reporting data. HUD may not collect this information, and respondents are not required to complete this form, unless it displays a currently valid OMB Control Number.

GRANTEE & REQUESTOR INFORMATION

REQUEST TYPE	Role to be Performed by Headquarters	Role to be Performed by Field or Local IDIS Administrator
	New Request ☐	Drop from IDIS ☐
	Renew Lapsed ID ☐	Change Function or Program Area ☐
	Change Name ☐	
	Add Access for Another Grantee ☐	

Please create a five digit pin that will be used for password resets. [ ] [ ] [ ] [ ] [ ]

Requestor's Name (Last, First, MI): Office E-mail Address:

Office Address: Office Phone: ext.:

Grantee Name in IDIS: **GRANTEE TYPE**
City ☐ County ☐ State ☐ Non-Profit ☐ Sub Grantee* ☐

Please Mark All Necessary Functions & Programs

Authorized Functions: Set Up Activity ☐ Request Drawdown ☐ Approve Drawdown ☐ Local IDIS Administrator ☐

Program Areas: CDBG ☐ HOME ☐ ESG ☐ HOPWA ☐ HESG ☐ HOPWA-C ☐ Other: _____
If other, please specify name of program

*Approval of State Sub Grantee Request – CPD State Coordinator or State Official name, signature and date:
Name: Signature: Date:

Modules

Con Plan:	Create/Edit/Submit ☐	Edit ☐	View ☐
Caper:	Create/Edit/Submit ☐	Edit ☐	View ☐

IDIS Online Rules of Behavior
September 14, 2015

Introduction

This Rules of Behavior (RoB) procedure was developed as a guide to ensure that all users of IDIS Online are made aware of their security responsibilities before accessing IDIS Online. The RoB defines responsibilities and procedures for secure use of IDIS Online. By reading and acknowledging these rules, users accept the responsibility to protect IDIS Online and data. Users are accountable for their actions and the requirements to protect IDIS Online data and equipment from both malicious and accidental loss and damage. These rules clearly delineate the responsibilities of and expectations for all individuals with access to IDIS Online. Non-compliance with these rules will be enforced through sanctions commensurate with the level of infraction.

Responsibilities

All authorized users who have access to IDIS Online are required to read, acknowledge understanding, and sign the RoB before accessing IDIS Online and associated data. This acknowledgement must be completed annually thereafter.

By agreeing to and signing these rules, the user signifies:

1. Understanding that access is given only to IDIS Online to which the user requires access in the performance of their official duties and the user will not attempt to access systems they are not authorized to access.

2. Understanding of the IDIS Online Rules of Behavior (IDIS RoB) security requirements.
3. Acknowledgement that disciplinary action may be taken based on violation of the IDIS RoB.

The IDIS Online System Security Administrator (SSA) verifies that the users who require access to IDIS Online have read and accepted (via signature on the acceptance form) this IDIS RoB.

Other Policies and Procedures

This IDIS RoB is intended to enhance and further define the specific rules each user must follow while accessing IDIS Online. The rules are consistent with the policy and procedures described in the following directives:

Revision of OMB Circular No. A-130, Transmittal No. 3, Appendix III, "Security of Federal Automated Information Resources."	https://www.whitehouse.gov/omb/circulars_a130_a130pre
Privacy Act of 1974, as amended, 5 U.S.C. § 552a	http://www.justice.gov/opcl/privacy-act-1974
18 USC 1030(a)4, "Accessing to Defraud and Obtain Value	http://www.gpo.gov/fdsys/granule/USCODE-2010-title18/USCODE-2010-title18-partI-chap47-sec1030/content-detail.html
NIST Special Publication 800-18 - Revision 1, Guide for Developing Security Plans for Information Technology Systems, February 2006	http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
HUD Information Technology Security Policy Handbook	http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25

Application Rules

Because written guidance cannot cover every contingency, you are asked to go beyond the stated rules, using your best judgment and highest ethical standards to guide your actions. These rules are based on Federal laws and regulations and HUD policies. As such there are consequences for non-compliance. The following IDIS RoB is the minimum rules for users who are requesting an IDIS Online user account:

1. You are aware of the existence of and penalty for violating 18 USC 1030 and abide by:
    a. The elements of 18 USC 1030(a)4, "Accessing to Defraud and Obtain Value" are:
        i. Knowingly accessing a protected computer without or in excess of authorization;
        ii. With intent to defraud;
        iii. Access furthered the intended fraud; and
        iv. Obtain anything of value
    b. The penalty for violating this statute includes a fine and imprisonment of not more than ten years, or both.
2. You must adhere to HUD's policy requiring a separation of duties between the requestor and approver for financial transactions:
    a. Effective December 14, 2001, the same person can no longer both request and approve a given draw down in IDIS Online.
    b. While individual persons may have the power to both request and approve draws, this rule prevents an individual from approving a draw that he or she created. IDIS Online requires two people to be involved in every draw down of funds.
3. Currently, the IDIS Online Local Administrator initially defines what a person can do in IDIS Online, carrying out the wishes of each grantee's authorizing official — mayor, grant holder, CEO, CFO, etc. Some users have full rights, while others have limited rights of various kinds. You understand that you are given access only to IDIS Online to which you require access in the performance of your official duties and that you will not attempt to access systems that you are not authorized to access.
4. You are prohibited from misusing IDIS Online, i.e., exceeding your authority. Your level of access to IDIS Online is limited to ensure your access is not more than necessary to perform your legitimate tasks or assigned duties. If you believe you are being granted access that you should not have, you must immediately notify the IDIS Online SSA via email at IdisUseridRequests@hud.gov.
5. You must immediately notify your Supervisor, CPD Field Office Administrator, and/or your Local Grantee Administrator if your access/privilege are no longer required, termination, promotion, and transferred.
6. You must maintain the confidentiality of your authentication credentials such as your password. Do not reveal your authentication credentials to anyone and do not record passwords on paper or in electronic form.
7. You must report all security incidents or suspected incidents (e.g., lost passwords, improper or suspicious acts) related to IDIS Online to the HUD Computer Incident Response Team at CIRT@hud.gov.
8. Your IDIS Online password expires every 90 days, so ensure you access IDIS at least once a month. Users who do not use IDIS within a 90 day period will find their accounts are de-activated.

9. You must follow proper logon/logoff procedures. You must manually logon to your session; do not store your password locally on your system or utilize any automated logon capabilities. You must promptly logoff when session access is no longer needed. If a logoff function is unavailable, you must close your browser. Never leave your computer unattended while logged into IDIS Online.
10. You must not establish any unauthorized interfaces between IDIS Online and other non-HUD systems.
11. Your access to IDIS Online constitutes your consent to the retrieval and disclosure of the information within the scope of your authorized access, subject to the Privacy Act, and applicable Federal laws.
12. You must safeguard IDIS Online resources against waste, loss, abuse, unauthorized use of disclosure, and misappropriation.
13. You must not process classified national security information on IDIS Online.
14. You must not browse, search or reveal IDIS Online data except in accordance with that which is required to perform your legitimate tasks or assigned duties. You must not retrieve data, or in any other way disclose data, for someone who does not have authority to access that information.
15. By your signature or electronic acceptance (such as by clicking an acceptance button on the screen), you must agree to these rules

User Acknowledgement and Certification— I acknowledge and certify that:

1. I understand the IDIS RoB and Federal Government policies as set forth above regarding security awareness and practices when accessing and utilizing IDIS Online.
2. I have read and understand the IDIS RoB governing my use of IDIS Online and agree to abide by them.
3. I understand my responsibilities and the penalties for NOT ADHERING to the IDIS RoB.
4. I understand that failure to comply will result in disciplinary action against me which may include, but are not limited to, a verbal or written warning, removal of system access, reassignment to other duties, demotion, suspension, reassignment, termination, and possible criminal and/or civil prosecution.

Requestor Name: **Signature:** **Date:**

GRANTEE APPROVING OFFICIAL

Approving Official's Name:

_____

Title:

_____

Office Phone: ext.:

_____

Office Address: (Street, City, State, Zip)

_____

_____

Signature: _____ Date: _____

I authorize the person above to have access to IDIS functions checked.

NOTARY

The Approving Official's signature must be notarized to verify the identity of the individual who signed this document using the appropriate notary certificate of the state, territory or insular area. Once completed, attach the completed notary certificate to this form and send to your local HUD CPD Field Office. If your state, territory or insular area does not require a notary certificate, use the space below.

Date: _____

Signature: _____

HUD FIELD OFFICES

Field Office Approval (CPD Director or Designee)

Name: Signature: Date: