U.S. Department of Housing and Urban Development
Departmental Rules of Behavior for Use of Information Resources
Annual Acknowledgement

The U.S. Department of Housing and Urban Development (HUD) Departmental Rules of Behavior (RoB) for Use of Information Resources (HUD RoB) provides the rules that govern the appropriate use of all HUD information resources for Department users, including federal employees, contractors, and other system users. These rules are based on Federal laws and regulations, and HUD policies.

All users of HUD information resources must read the HUD RoB and sign the accompanying acknowledgement annually, which may be done as part of the annual HUD Security Awareness Training. By signing the form users reaffirm their knowledge of, and agreement to adhere to, the HUD RoB. The HUD RoB may be presented to the user in hardcopy or electronically. The user's acknowledgement may be obtained by written signature or, by electronic acknowledgement or signature.

The HUD RoB cannot account for every possible situation. Therefore, you are asked to go beyond the stated rules, using sound judgment and the highest ethical standards to guide your actions and decisions.

Non-compliance with the HUD RoB may be cause for disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include one or more of the following actions:

- Suspension of access privileges;
- Revocation of access to federal information, information systems, and/or facilities;
- Reprimand;
- Termination of employment;
- Removal or disbarment from work on federal contracts or projects;
- Monetary fines; and/or
- Criminal charges that may result in imprisonment.

Acknowledgement and Acceptance

I acknowledge that I have read the above HUD's Departmental Rules of Behavior for Use of Information Resources. I understand, accept, and agree to comply with all terms and conditions of these Rules of Behavior.

Name Print: _____

Name Sign: _____

Date: _____

CONTINUE BELOW

RULES OF BEHAVIOR

a. I shall only access Departmental information and information resources that I am required to access to perform my official government duties, and I will not attempt to access systems and information that I am not authorized to access.

b. I understand that I have no expectation of privacy while accessing Departmental information or information resources.

c. I understand that I shall be held accountable for my actions while accessing and using Departmental information or information resources.

d. I shall behave in an ethical, informed, and trustworthy manner.

e. I understand that any breach of the Departmental Rules of Behavior shall be considered an adverse security event. If the event is deemed willful, it will be escalated to a computer security incident, which is defined as a violation of policy. Depending on the security incident and the specific information involved, disciplinary action for the violation may consist of a letter or warning/caution, revocation of access to the Departmental information and information resources, reassignment or demotion, suspension or removal from Federal Service, and/or found guilty of a misdemeanor punishable by fines of $5,000.

f. I shall immediately report suspected or identified security and privacy incidents or any incidents of suspected fraud, waste or misuse of HUD information resources to the HITS National Help Desk at (888) 297-8689.

g. I shall immediately report the loss or theft of any Departmental information technology resource to the HITS National Help Desk at (888) 297-8689.

h. I shall complete the annual HUD Information Technology Security Awareness and Privacy Act training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

i. I understand that HUD's Departmental Rules of Behavior identify the minimal rules with which I must comply.

j. I understand that my refusal to sign HUD's Departmental Rules of Behavior may have an adverse impact on my employment with the Department or result in denied access to HUD information and information resources.

k. I shall follow established procedures for requesting access to Departmental information resources and for notifying appropriate parties when access is no longer needed.

l. I shall comply with and follow established HUD information technology security and privacy policies and procedures.

m. I shall only use systems, software, and data for which I am authorized and use them

only for official government business

n. I agree to comply with all software licensing agreements and not violate Federal copyright laws.

o. I shall not install unauthorized software (this includes software available for downloading from the Internet or personally owned software) on Departmental information resources.

p. I shall comply with the Limited Personal Use of Government Office Equipment Policy, as identified in HUD Handbook 2400.1, Chapter 8.

q. I shall protect sensitive information from disclosure to unauthorized persons or groups.

r. I shall properly dispose of HUD sensitive information, either in hardcopy, softcopy or electronic format, in accordance with HUD policy and procedures.

s. I shall not circumvent or attempt to circumvent any security countermeasures or safeguards.

t. I shall not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
I shall not share identification or authentication materials of any kind, nor allow any other person to access or use any HUD information technology resource by employing my account and password information.

v. I shall choose passwords that comply with HUD's established password rules established for Departmental systems and applications.

w. I shall protect passwords and access numbers from disclosure. I shall not record passwords or access control numbers on paper or in electronic form. I will ensure that I log off or lock any computer or console before walking away and will not allow another user to access that computer or console while I am logged on to it.

x. I shall comply with the requirement that sensitive information stored on any computer or electronic device used in a residence or on travel shall be encrypted, as required by HUD Handbook 2400.25, Information Technology Security Policy.

y. I shall not access, transmit or store remotely any HUD sensitive information that is not encrypted, as required by HUD Handbook 2400.25, Information Technology Security Policy.

z. I shall obtain the approval of appropriate management officials before releasing HUD information for public dissemination.

aa. I shall protect Government property from theft, loss, destruction, or misuse. I will follow HUD policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer

required for HUD activities.

bb. I shall not disable or degrade software programs used by HUD that install security software updates to HUD computer equipment, to computer equipment used to connect to HUD information systems, or to create, store or use HUD information.

cc. I shall only use HUD-approved remote access solutions to telework or remotely access HUD information and shall safeguard all sensitive information accessed in this manner

dd. I shall adhere to all provisions or agreements related to teleworking or working remotely.

ee. I shall physically protect laptop computers and any other mobile device and air cards from theft and shall be particularly aware of the threat of loss during periods of travel.

ff. I shall not allow sensitive information to reside on non-HUD systems or devices unless specifically designated and approved in advance by the appropriate management official.

gg. I shall not enter unauthorized, inaccurate, or false information into a HUD information resource.

hh. I understand that I may be required to acknowledge or sign additional specific or unique Rules of Behavior in order to access or use specific HUD systems. I understand that those specific rules of behavior may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.