RULES OF BEHAVIOR FOR
TENANT RENTAL ASSISTANCE CERTIFICATION SYSTEM
(TRACS – F87) Internal/External Users
and
MULTIFAMILY ENTERPRISE INCOME VERIFICATION (MF EIV) SYSTEM
Internal Users

Internal Users

(If your User ID begins with the letter **"H"** or letter **"C"**, then you are an INTERNAL user.)

- Complete the Access and Security Training requirements identified on the TRACS website at http://hudatwork.hud.gov/HUD/housing/po/h/hm/tracs/trxhome
- Read the following Rules of Behavior (ROB), check the certification checkbox, and click the Accept button at the bottom of the page to continue (or Logout without using the system if you do not agree to ROB.)
- Print, sign, and scan the ROB to a PDF and email to MF.TRACS.RECERT@hud.gov

External Users

(If your User ID begins with the letter **"M"** or letter **"I"**, then you are an EXTERNAL user.)

- Complete the Access and Security Training requirements identified on the TRACS website at http://portal.hud.gov/hudportal/HUD?src=/program_offices/housing/mfh/trx/trxsum
- Read the following Rules of Behavior (ROB), check the certification checkbox, and click the Accept button at the bottom of the page to continue (or Logout without using the system if you do not agree to ROB.)
- Print, sign, and *retain a copy of the ROB for your records.*

External Users Only: DO NOT SEND A COPY OF THE ROB TO HUD UNLESS REQUESTED!

RULES OF BEHAVIOR

Internal/External HUD Users:

The Office of Multifamily Housing (MF) may grant system access to internal users (HUD employees, contractors) and external users (owners of multifamily property, management agents, contract administrators, service bureaus and clients/customers) who have a need to utilize the TRACS –F87 system or internal users who have a need to utilize the MF EIV system for **official HUD business only**. Access is based on specific job function, and only information to which you are authorized will be accessible.

The system user identification (User ID/password) issued to you are to be used solely in connection with the performance of your responsibilities in support of the HUD mission and may not be used for personal or private gain. As a condition of receiving access, you agree to be responsible for the confidentiality of the assigned information (i.e., will not provide to anyone), accountable for all activity with your user identification, and that you will notify the MF TRACS Security Office (MFTRACSSECURITY@hud.gov, include User ID) in writing upon leaving your place of employment or transfer to another position/office.

Additional rules of the system follow:

a) Log off or lock the system when leaving the system/workstation area.
b) Refrain from leaving written passwords in the workstation area.
c) Passwords must be changed every 30 days (iMAX and TRACS Web). Avoid creating passwords that can be easily associated with you.
d) Your User ID will be suspended after 90 days of inactivity and you will have to request re-activation of access (iMAX, TRACS Web-based Applications including MF EIV).
e) Avoid posting printouts of sensitive output data on bulletin boards.
f) Control input documents by returning them to files or forwarding them to the appropriate contact person in your office.
g) Avoid violation of the Privacy Act, which requires confidentiality of personal data contained in government and contractor data files. Penalties apply to the misuse of data.
h) Protect all electronic /optical media and hardcopy documentation containing sensitive information and properly dispose of it by shredding hardcopy documentation.
i) Avoid saving sensitive HUD information on the local drive of a laptop, personally-owned computer or other mobile or portable technology (“flash drives”, removable/external hard drives, etc.)
j) Report security violations immediately to the HUD’s Call Center at 1-888-297-8689.
k) Cooperate in providing personal background information to be used in conducting security background checks required by Federal regulations.
l) Respond to any requests for information from either the Government Technical Representative, MF TRACS Security Office or management officials regarding system security practices.
m) Review the Department’s “Information Technology Security Policy 2400.25” and other security guidance at: http://portal.hud.gov/hudportal/documents/huddoc?id=240025CIOH.pdf

Internal HUD Users Only:

n) Your User ID will be suspended after 45 days of inactivity and you will need to contact the Information Security staff at 1-888-297-8689 (Option 3) for a password reset **(TRACS Mainframe**).
o) Your User ID will be terminated after six months of inactivity, and you will need to re-apply for access to the system **(TRACS Mainframe).**
p) Individuals who telework or remotely access HUD/TRACS information should do so only through approved remote access solutions (as hudmobile.hud.gov) and should safeguard all sensitive information accessed in this manner. Remote access users will also adhere to Rules of Behavior for Remote Access.

USER AGREEMENT AND CERTIFICATION

Actions violating any of these rules will result in immediate termination of your assigned User ID/ password from the system(s) and can result in further disciplinary action (civil or criminal) as prescribed by the Office of the Inspector General.

- **Unauthorized disclosure** can result in a felony conviction and a fine of up to $5,000 and/or imprisonment up to five (5) years, as well as civil penalties.
- **Unauthorized inspection** of data can result in a misdemeanor penalty of up to $1,000 and/or one (1)-year imprisonment, as well as civil penalties.

CERTIFICATION: I have read the above statement of policy regarding system security awareness and practices when accessing HUD's information resources. I understand the Department's policies as set forth above, and I agree to comply with these requirements as a condition of being granted limited access to the Multifamily Housing information technology resources. I further certify that I have completed or will complete the Security Training requirements identified on the TRACS website within 30 days**.**

EXTERNAL USERS: (1) SIGNED TRACS RULES OF BEHAVIOR and (2) SECURITY AWARENESS TRAINING CERTIFICATE MUST BE AVAILABLE UPON REQUEST AND ARE SUBJECT TO REVIEW OR AUDIT AT ANY TIME BY HUD STAFF AND/OR HUD REPRESENTATIVES WITH OVERSIGHT AND MONITORING RESPONSIBILITIES.

________________________________ ____

System User's Name (print) System User's Name (signature)

User Id: _________________________ Date Signed: _____________________________

Appendix A: Rules of Behavior

HUD Information Technology (IT) developed a written set of Rules of Behavior for all users of application systems. The Information Security Guide addresses limitations on changing data, searching databases, and divulging information. The Rules of Behavior state disciplinary action may result from violation of policies. A copy of the Rules of Behavior is included in Appendix C.

HUD users (M&M contractors, HOC, NSC, HUD HQ, and OIG) are required to comply with the rules detailed in HUD's Computer Security Policy Handbook 2400.25. Registered brokers are required to comply with the requirements of the Officer Next Door/Teacher Next Door Program. The login page presents individuals and brokers with this warning:

> Submission of a bid from a party other than a qualified officer/teacher or a broker acting on behalf of a qualified officer/teacher on an Owner-Occupant Priority property, knowing the same to be false, subjects the person placing the bid to a possible $250,000 fine or two years' imprisonment or both, as per the HUD Sales Contract Conditions of Sale.

1. Responsibilities

Office of Management and Budget (OMB) Circular A-130 Appendix III requires every System Security Plan (SSP) to contain a Rules of Behavior (ROB). ROB apply to the system users and list specific responsibilities and expected behavior of all individuals with access to or use of the named information system. In addition, ROB outlines the consequences of non-compliance and/or violations.

Why are Rules of Behavior Needed?

ROB is part of a complete program to provide good information security and raise security awareness. ROB describes standard practices needed to ensure safe, secure, and reliable use of information and information systems.

Who is covered by the Rules of Behavior?

The ROB covers all government and non-government users of the named information systems. This includes contract personnel and other federally funded users.

What are the Consequences for Violating the Rules of Behavior?

Penalties for non-compliance 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.

2. Application and Organization Rules

A. *Passwords*

1. Passwords should be a minimum of eight characters, and be a combination of letters, numbers and special characters (such as *#$ %). Dictionary words should not be used.
2. Passwords will be changed at least every 90 days and should never be repeated. Compromised passwords will be changed immediately.
3. Passwords must be unique to each user and must never be shared by that user with other users. For example, colleagues sharing office space must never share each other's password to gain system access.
4. Users who require multiple passwords should never be allowed to use the same password for multiple applications.

5. Passwords must never be stored in an unsecured location. Preferably, passwords should be memorized. If this is not possible, passwords should be kept in an approved storage device, such as a Government Services Administration Security Container. If they are stored on a computer, this computer should not be connected to a network or the Internet. The file should be encrypted.

B. Encryption

1. Extremely sensitive data should be encrypted prior to transmission.
2. The sensitivity of the information needing protection, among other considerations, determines the sophistication of the encryption technology. In most circumstances, only the most sensitive or compartmentalized information should be encrypted.
3. Files that contain passwords, proprietary, personnel, or business information, and financial data typically require encryption before transmission, and should be encrypted while stored on the computer's hard disk drive.
4. Sensitive information that travels over wireless networks and devices should be encrypted.

C. Internet Usage

1. Downloading files, programs, templates, images, and messages, except those explicitly authorized and approved by the system administrator, is prohibited.
2. Visiting websites including, but not limited to, those that promote, display, discuss, share, or distribute hateful, racist, pornographic, explicit, or illegal activity is strictly prohibited.
3. Because they pose a potential security risk, the use of Web based instant messaging or communication software or devices are prohibited.
4. Using the Internet to make non-work related purchases or acquisitions is prohibited.
5. Using the Internet to manage, run, supervise, or conduct personal business enterprises are prohibited.

D. Email

1. Except for limited personal use, non-work-related e-mail is prohibited. The dissemination of e-mail chain letters, e-mail invitations, or e-mail cards is prohibited.
2. E-mail addresses and e-mail list-serves constitute sensitive information and are never to be sold, shared, disseminated, or used in any unofficial manner.
3. Using an official e-mail address to subscribe to any non-work related electronically distributed newsletter or magazine is prohibited.

E. Working from Home/Remote Dial-up Access

1. Users may dial into the network remotely only if pre-approved by the system administrator.
2. Users must be certain to log-off and secure all connections/ports upon completion.
3. Users who work from home must ensure a safe and secure working environment free from unauthorized visitors. At no time should a "live" dial-up connection be left unattended.
4. Web browsers must be configured to limit vulnerability to an intrusion and increase security.

5. Home users connected to the Internet via a broadband connection (e.g. DSL or a cable-modem) must install a hardware or software firewall.
6. No official material may be stored on the user's personal computer. All data must be stored on a floppy disk and then secured in a locked filing cabinet, locker, etc.
7. Operating system configurations should be selected to increase security.

F. Unofficial Use of Government Equipment

Except for limited personal use, government equipment including, but not limited to, fax machines, copying machines, postage machines, telephones, and computers are for official use only.

G. Other Rules of Behavior

1. Using system resources to copy, distribute, utilize, or install unauthorized copyrighted material is prohibited.
2. Users who no longer require IT system access (as a result of job change, job transfer, or reassignment of job responsibilities) must notify the system administrator.
3. When not in use, workstations must be physically secured. Users must also log-off or turn-off the system.
4. Screen-savers must be password protected.
5. Movable media (such as diskettes, CD-ROMs, and Zip disks) that contain sensitive and/or official information must be secured when not in use.
6. Altering code, introducing malicious content, denying service, port mapping, engaging a network sniffer, or tampering with another person's account is prohibited.
7. If a user is locked out of the system, the user should not attempt to log-on as someone else. Rather, the user should contact the system administrator.

H. Additional Rules of Behavior for System Administrators

1. System administrators may only access or view user accounts with the expressed consent of the user and/or management.
2. System administrators may not track or audit user accounts without the expressed consent of the user and/or management.
3. System administrators must make every reasonable effort to keep the network free from viruses, worms, Trojans, and unauthorized penetrations.
4. It is the system administrators' responsibility to account for all system hardware and software loaned to system users for the execution of their official duties.