

Rules of Behavior for the RAD Resource Desk

This computer system, including all related equipment, networks, and network devices (specifically including Internet access) contains data belonging to the U.S. Department of Housing and Urban Development, and is provided for authorized U.S. Government use only. By logging onto the RAD Resource Desk, you agree to abide by the policies below. Security policy emphasizes awareness practices for the purpose of safeguarding HUD's information resources.

The system user identification (USERID) and password issued to you are your means to access these resources. They are to be used solely in connection with the performance of your responsibilities as set forth in your job description, contract or agreement(s) with RAD and HUD. Use by anyone other than yourself is expressly prohibited. You agree to be responsible for the confidentiality of the assigned information and accountable for all activity with your USERID. Further, you agree that you will not provide this confidential USERID/password to another user nor will you sign on to HUD systems so that another person may access or operate the workstation in your absence or on your behalf. ***Actions of this type constitute a breach of system security and will result in immediate termination of your assigned USERID/password from the system.***

In addition, you agree to:

- (a) Log-off the system when leaving the system/workstation area;
- (b) Refrain from leaving written passwords in the workstation area;
- (c) Avoid creating a personal password that can be easily associated with you;
- (d) Avoid posting printouts of sensitive output data on bulletin boards;
- (e) Avoid leaving system output reports unattended or unsecured;
- (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;
- (h) Avoid uploading documents that contain Personally Identifiable Information (PII), such as Social Security Number, date of birth, etc.
- (i) Immediately contact the HUD Inspector General's Office, as appropriate, regarding any suspected violation or breach of system security;

- (j) Respond to any inquiries and requests for information you may receive from either the HUD Headquarters or management officials regarding system security practices;
- (k) 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.);
- (l) If sensitive data must be stored on any type of HUD-approved mobile/portable technology (laptops, removable hard drives, “flash drives”, etc.), ensure that it is protected via encryption; and
- (m) Support the Resource Desk's vulnerability disclosure program by directing any reports of system vulnerabilities to resourcedesk@radresource.net.