Rules of Behavior for HUD Systems

**The U.S. Department of Housing and Urban Development** has granted access to you to utilize the Department's automated information resources. However, as a condition of receiving this access, you are required to be aware of the Department's system security policies and to abide by these policies. Security policy emphasizes awareness practices for the purpose of safeguarding the Department's valuable 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 the Department. 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 user identification (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) Immediately contact the HUD Inspector General's Office, as appropriate, regarding any suspected violation or breach of system security;
* (i) Cooperate in providing personal background information to be used in conducting security background checks to the extent required by Federal regulations;
* (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) Protect all electronic/optical media and hardcopy documentation containing sensitive information and properly dispose of it by shredding hardcopy documentation, or by contacting the HITS Help Desk to dispose of electronic/optical media.
* (l) 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.).
* (m) 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.
* (n) Individuals who telework or remotely access HUD information should do so only through approved remote access solutions (such as hudmobile.hud.gov), and should safeguard all sensitive information accessed in this manner