Office of Public Housing and Voucher Programs

Safeguarding Privacy-Protected and Sensitive Data

Storing Sensitive Data in Electronic Formats

a. **Enable Windows logon** to password protect PCs and laptops containing sensitive data;

b. **Encrypt all data on mobile computers/devices** (e.g., laptops, pocket PCs, CDs, flash drives, etc.), which carry agency data unless the data is determined to be non-sensitive, in writing, by your information security officer or his/her designate. Data must be encrypted using the triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES) algorithms. However, when possible, AES should be used as it is expected that 3DES will be phased out;

Storing Hard Copies

a. When traveling with hard copies containing sensitive data for RIM reviews, the **hard copies must remain with you at all times**. Hard copies should not be left unattended, where the information is not secure.

b. **Hard copies must have the cover sheet** to prevent unauthorized viewing of data.

c. **Once the RIM/UIV reviews have been completed and Corrective Action Plans have been satisfied, the Appendix A and spreadsheet documents must be destroyed in such a manner that all sensitive information on that media cannot be recovered by ordinary means**. Examples of appropriate methods are crosscut shredders, degaussing, and approved disk-wiping software. The RIM reviewer may wish to scan the Appendix A documents for archiving purposes, but the reviewer must follow the guidelines for "***Storing Sensitive Data in Electronic Formats***" (see above).

Note: At the conclusion of the RIM/UIV review, prior to e-mailing the Tenant Error File Report to HUD Headquarters, the file must be encrypted. Please see the "Instructions for Zipping and Encrypting Files" document.