Data Destruction Policy and Procedures

Policy

When a Restricted Data Agreement (RDA) is terminated, the Health and Retirement Study requires that the researchers who were authorized to use restricted data products must certify that they have destroyed:

- Physical media on which the restricted data products were distributed.
- Derived copies of all restricted data files. This may require destruction or secure erasure of the storage device(s) on which the derived files are stored.
- Other materials, which include (but are not limited to) backup media, printed listings, and lab notes.

Destruction Procedures

All restricted data files (e.g., all copies of the original restricted data and of all files derived in whole or in part from the restricted data) must be destroyed when the RDA is terminated. There are multiple approaches that can be taken to make such files inaccessible. Restricted data users should choose one of the options listed below:

1. Physical destruction of the device(s) (e.g., CDs, DVDs, tapes, diskettes) on which the restricted data files were stored. *This is a recommended solution.*
2. Secure erasure of storage media followed by reformatting. *This is a recommended solution.*
3. Secure deletion of **individual** folders and/or files. *This is **not** a recommended solution and will require special permission from the Health and Retirement Study.*[1]

After completion of one of the above three destruction procedures, the researcher team must submit an HRS Restricted Data File Destruction Certification form to HRS.

Special rules for solid-state-drive (SSD) devices:

Sanitizing data stored on SSD media requires the use of special techniques that differ from those used for magnetic storage devices, as outlined in the research work of Michael Wei et al. at University of California, San Diego.[2] Although SSD devices have built-in commands for data erasure[3], this technique may not be totally effective[4] in the context of data security.[5] As a result, the Health and Retirement Study recommends **cryptographic erasure** as a solution for removal of restricted data from an SSD device. Cryptographic erasure requires that you implement disk encryption at the beginning of the project. Please plan accordingly so that your device need not be destroyed at the end of your project. Steps involved are:

1. Implement whole disk encryption; save keys.
2. Carry out secure data work.
3. At end of project, delete keys.
4. Reformat SSD.

[1] Secure deletion of individual folders and files is complicated by the need to find and erase temporary copies of restricted files that are created by the operating system during normal use. For example, computer memory paging may produce files that contain restricted data. (http://ultraparanoid.wordpress.com/2007/09/19/securely-erase-individual-files/)

[2] *Sanitizing Solid-State Storage Devices* http://nvsl.ucsd.edu/index.php?path=projects/sanitize

[3] For example, the Security Erase Unit (SEU) command erases all LBAs [logical block addresses], thus deleting the links that define where data elements are stored. The problem is that the actual data may remain on the drive.

[4] *Erasing SSDs: Security is an issue*, Michael Kassner, February 13, 2014, http://www.techrepublic.com/article/erasing-ssds-security-is-an-issue/

[5] *Can data stored on an SSD be secured?* Lucas Mearian, Computerworld, February 28, 2011 http://www.computerworld.com/s/article/9211519/Can_data_stored_on_an_SSD_be_secured_

Additional Information

How-to Information

- Overview of secure data deletion methods (University of Pennsylvania).
- Secure Data Deletion and Media Disposal (University of Michigan) .
- Secure Data Deletion (University of Minnesota) .
- Data deletion for printers, copiers and multi-function devices (University of Minnesota).
- Overview of secure data deletion methods (University of Pennsylvania).
- Secure Deletion of Data from Magnetic and Solid-State Memory, Peter Gutmann, Department of Computer Science, University of Auckland. The article is interesting for historical reasons; read the epilogue and recommendations for information on current deletion methods.

Total Disk Wipe - All Platforms

- DBAN (Darik's Boot And Nuke) – an open-source boot disk utility that deletes the contents of any detected hard disks. (Note: This utility can also be used to delete specific files and folders.)
- Physical destruction – Use a commercial solution such as Shred-it or remove the drive and hit it with a sledgehammer.

Selective File Wipe - Windows

- Wipe File - Portable application that overwrites the specific disk space occupied by the file you'd like erased and leaves the rest of the disk untouched.
- DeleteOnClick - Integrates with the Windows shell, adding a "Securely Delete" option to the right click menu which engages a Department of Defense 5220.22-M over-write on the files.
- Eraser - In addition to securely deleting individual files, Eraser can be scheduled to perform regular overwrites of empty disc space ensuring you catch those orphan files hanging outside the reach of Windows.
- SDelete - Allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk (Microsoft/SysInternals). Runs on Windows XP and higher (clients) and Windows Server 2003 and higher.

Selective File Wipe - Mac OS X

- Permanent Eraser - Although Mac users have had the "secure empty trash" option, based on a multiple pass DoD method, since OS 10.3, Permanent Eraser offers peace of mind for those needing more assurance.

Selective File Wipe – Linux/Unix

- wipe – A unix command designed to securely erase files from magnetic media.
- shred – Linux/Unix file over-write/delete command.

SSD Information

- Archlinux: SSD Memory Cell Clearing
- Kingston Technology white paper: SSD Data Wiping: Sanitize or Secure Erase SSDs?
- Michael Wei, et al., Reliably Erasing Data from Flash-Based Solid State Devices
- Non-volatile Systems Laboratory, Sanitizing Solid-State Storage Devices