Agencies must establish formal, documented media disposal procedures. Documented procedures are critical, as they help ensure that effective processes are consistently applied, regardless of staffing changes or turnover.

While the OCIO IT Security Standards provide some latitude on how the requirements in Section 8.3, Media Handling and Disposal, can be met, there are many best practices that agencies can adopt to ensure they are protected from unauthorized access to agency data. In addition, agencies should be mindful of the data retention requirements for any data contained on storage media to be disposed.

Maintain secure control and custody of media to be disposed

- Media to be disposed must stay within the control of the agency from the time it is collected to the time it is sanitized.
- Pick-up/Transit ? Storage media to be disposed should be collected by, and in the constant possession of dedicated, trusted personnel
- Media should be maintained in a secure, locked area until it can be sanitized

Render *all* data on the media unusable

When files are deleted from a computer, emptied from the Recycle Bin or even by reformatting, if it is not overwritten it can be easily recovered using commonly available tools.

- Don?t delete the data ? destroy it
- All data should be rendered unusable using special software designed for this purpose (See examples at bottom of page)
- Meets the requirements of Section 8.3 of the OCIO IT Security Standards

Physical destruction is an option

- Agencies may physically destroy the media itself rather than sanitize the media
- This typically takes the form of shredding or pulverization, ensuring the media can never be used again.
- Any media that cannot be sanitized through the use of software tools must be physically destroyed.

Private companies are available to perform this service, and agencies must be sure that they can maintain control of the media from the time it leaves the agency until the time it is actually destroyed. When pursuing this option, agencies should consider those companies that dispose or recycle these materials in an environmentally responsible way.

Keep Detailed Records

Agencies should maintain records that document all media disposal activities, as this can provide agencies with the means of confirming that specific media was disposed of properly if it is later called into question.

Records for disposed media should include:

- Information about the media (type, serial number, other unique identifiers)
- The date the media was sanitized
- The person performing the activity
- The method used to render all data unusable (e.g. software tool used or physical destruction of the media)
- The signature of the person responsible for ensuring that all data on the storage media has been rendered unusable.

Provide evidence of disposal

In addition to keeping records, it is a good idea to identify media that has been sanitized. This can include:

- Affixing a sticker or a document to the device or CPU indicating that the data sanitation process was completed. This helps agencies easily identify and segregate machines internally, and lets others, such as DES Surplus, know that the media has been wiped and can be made available for use by others.

Free Data Erasure Software

Free software utilities that can be used to meet OCIO IT Security Standards data and media disposal requirements:

Active@KillDisk - http://www.killdisk.com [1]

- Data Sanitization Methods: DoD 5220.22-M, GOST p50739-95, NSA 130-2, Schneier, Gutmann, 21 -23 NIST 800-88, Random Data, Write Zero

Eraser Portable - http://portableapps.com/apps/security/eraser-portable [2]

- Data Sanitization Methods: DoD 5220.22-M, AFSSI-5020, AR 380-19, RCMP TSSIT OPS-II, HMG IS5, VSITR, GOST R 50739-95, Gutmann, Schneier, Random Data

Microsoft?s SDelete - http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx [3]

- Data Sanitization Methods: DoD 5220.22-M, Gutmann, Random Data

Freeraser - http://download.cnet.com/Freeraser/3000-2144_4-10909403.html [4]

- Data Sanitization Methods: DoD 5220.22-M, Gutmann, Random Data

---

Source URL: https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets-3

Links:
[1] http://www.killdisk.com
[2] http://portableapps.com/apps/security/eraser-portable
[3] http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx
[4] http://download.cnet.com/Freeraser/3000-2144_4-10909403.html