MEDIA DISPOSAL GUIDELINES

Issued September 25, 2006, revised October 12, 2011, from Purdue University Security Officer's Group and IT Networks and Security. Questions about these guidelines can be addressed to itap-securityhelp@purdue.edu.

These guidelines are intended to support Purdue University’s Data Classification and Governance Policy (VII.B.6), as well as the Data Handling Requirements as issued by the University Data Stewards.

I. Disposal Guidelines for Paper-Based Media

1. The proper media disposal technique for any paper based documentation must match the highest classification of data that is contained in that document. Therefore, a document containing both University classified sensitive and restricted data must be disposed of in the manner required for the disposal of restricted data.

2. Existing Departmental Managers are responsible for overseeing paper-based document disposal in his or her area.

3. Destruction methods for paper-based documentation includes use of the Purdue University Confidential Material Recycling Program, and other methods such as shredding (cross-cut shredding is best), disintegration, incineration, and pulverization.

II. Disposal Guidelines for Electronic-Based Media

1. The proper media disposal technique for electronic storage devices depends whether or not the electronic storage media is being repurposed for University use.

2. Electronic Storage Devices Repurposed for University Use: If the physical media is going to be repurposed for University use, then the electronic storage device must be wiped with a multiple pass/DoD secure overwrite prior to being repurposed to another unit or area.

3. Electronic Storage Devices NOT Repurposed for University Use: If the physical media is not going to be repurposed for University use, then the electronic storage device must be physically destroyed.

4. Existing Departmental Managers are responsible for overseeing electronic storage device disposal in his or her area. This responsibility includes ensuring that appropriate multiple pass/DoD secure overwrites are properly completed and documented in the event that storage devices are repurposed for University use.
5. Multiple pass/DoD overwrite means to overwrite all addressable locations with a character, its complement, then a random character, and verify.

6. Physical destruction methods for electronic storage devices include use of the Purdue Recycling for the Future program. Other methods of physical destruction may be acceptable so long as the electronic storage device is destroyed and the data contained on that device may not be recovered by any means.

III. Related Documents
1. Purdue University Data Handling Requirements, available at: http://www.purdue.edu/securepurdue/bestPractices/dataClass.cfm


4. Purdue University Recycling for the Future media shredding program, available at www.purdue.edu/surplus (click on the Recycling for the Future link on the bottom of the page)


Revised November 21, 2011 to update URLs.
PURDUE UNIVERSITY
ELECTRONIC DATA DISPOSAL VERIFICATION

For information to be repurposed for University use, documentation confirming the multiple pass/DoD secure overwrite should be completed and maintained by the department performing the multiple pass/DoD secure overwrite. See sample form attached.

**Computer Ownership Information (Original Department):**

- Property Control #: ________________________________
- CPU Serial #: ________________________________
- Department: ________________________________
- Campus Telephone: ________________________________

**Computer Ownership Information (Transferee Department):**

- Department: ________________________________
- Campus Telephone: ________________________________

**Disk Wipe Information:**

- Date Cleaned: ________________________________
- Cleansing Method: ________________________________
- Cleaned By: ________________________________
- Campus Telephone: ________________________________