



Disposal of Desktop Media Containing Confidential or Sensitive Data

Last updated: 03/04/2007

In order to support various Purdue University auditing policies for confidential and sensitive data handling, IPFW IT Services End-User Support will perform the following procedures for supported desktops and laptops whenever warranted as below:

1. IPFW IT Services Help Desk maintains an optical shredder for destroying removable media that contains restricted or sensitive data. The shredder is available for use by supported departmental areas. The Departmental Coordinator or assigned responsible staff member is required to be present during the destruction of removable media.
 - a. For optical media: Run the CD or DVD through a CD shredder.
 - b. For floppy disk media: Break open the plastic shell, remove and shred the media surface.
 - c. For ZIP disk media: Break open the plastic shell, remove and shred the media surface.
 - d. For USB Flash Drive media: Break open the plastic shell, remove and physically break the memory SIMM or DIMM so that it is unusable.
2. IT Services End-User Support staff will sanitize desktop or laptop hard drives when machines are retired from use.
 - a. When a computer is removed from service, an IPFW IT Services staff person will bring it directly back to IPFW IT Services End-User Support offices and will begin the cleansing process of the hard drive(s) without losing sight of the system or by locking it up in a secured space.
 - b. The cleansing process will consist of using the GDISK WIPE utility that comes as part of our licensed Symantec Ghost software in Dept. of Defense mode.
3. IPFW IT Services End-User Support staff will ensure that any failed hard drive be cleansed or made unreadable.
 - a. Try the Ghost gdisk process above.
 - b. If step 3a is unsuccessful, physically take apart the drive and create a permanent crease in each of the platters.
 - c. If the failed hard drive is covered under warranty, the department will need to pay for the new drive or attest via email to the IPFW IT Services End-User Support Manager that guarantees the failed drive did not contain any confidential or sensitive data.

Loaner Equipment

- Since IPFW IT Services loaner equipment changes hands frequently, it is not feasible that hard drive media be cleansed to a "Department of Defense" standard between user changes.
- All IPFW IT Services users must complete and verify they have understood the **SS LAN Expectations Guidelines** (<http://www.purdue.edu/SSTA/workstationtechnology/customer/lanexpectations.php>) before being granted access to our systems.
- Item 2 on that list states that:
"Each user is expected to maintain the confidentiality of the data and use it only in conduct of University business."
- It is there implied that any IPFW IT Services supported user that utilizes loaner equipment, will abide by all Purdue Data Handling guidelines. Further information on that topic is found at:
<http://www.itap.purdue.edu/security/policies/guidelines.cfm>
- Users are responsible for deleting all data files from borrowed equipment prior to returning the equipment.