

Don't Forget the Data

Recycling Computers is Good, But What About Your Data?

More and more companies realize the need to implement a recycling program of some kind to deal with their outdated computer and technology-related equipment. Programs and Service Providers abound to take technology equipment away, disassemble it, thus reducing it to components that can be recycled into new products. But the question remains – what about your data?

The technicians responsible for refreshing computer systems generally do not have the bandwidth available to sanitize each and every hard drive before the computer recycler comes to pick up the equipment. And if they do have the time, is their process strenuous enough that they are certain each and every hard drive was sanitized? How is this task tracked? What quality assurance process is in place to insure 100% success of the data sanitization process?

Unlike a corporate IT Staff, an eGreen Certified Supplier has processes in place to insure your data is destroyed during the recycling process. If you've elected to have your computers prepared for resale, the eGreen Certified Supplier will destroy the data on the hard drive utilizing a disk wipe procedure that is verified by a separate team to insure complete erasure of data. On the other hand, if you've elected to have your computers completely recycled the eGreen Certified Supplier will physically remove the hard drive from the computer and destroy it by shredding. This too, is verified during the QA process.

There are three common methods for destroying data – physical destruction, disk wipe and degaussing. Of the three, physical destruction of the data media is by far the single most reliable way to assure that data is never accessed by anyone. The process physically shreds the data media into small particles, and the process can be used for any type of data media from hard drives to CDs and everything in between. Degaussing can be ineffective for drives such as large server drives encased in heavier metal than a typical PC hard drive or on RAID's.

Typical data media shredded are Hard Drives, CDs,

Diskettes, DVDs, Tape Media in all sizes, Cell Phones, Palm Pilots, PDAs, Black Berries – anything with data on it can be physically shredded if you have a large enough shredder.

Software Disk Wipe is specific to hard drives, and when used properly is a safe and effective way of destroying data. There are numerous applications for the “Disk Wipe” process, but generally the most recognized and secure method was developed by the Department of Defense (DOD) and is referred to as DOD Standards. The U.S. Department of Defense (DOD) 5220.22-M standard for disk-sanitization is one of the most rigorous disk wipe procedures there is. This wiping standard requires seven passes, with each pass formed of three different data wipes. The hard drive is rewritten and covered with random patterns. With each wipe, the deleted data becomes harder to piece back together.

The third type of data destruction, and least reliable, is degaussing which creates a high intensity magnetic field that is supposed to erase all magnetic recordings in a hard disk drive. Degaussing does destroy the data, but often after degaussing a hard drive is no longer useable. So if your recycling plans include reuse in any fashion of the hard drive, degaussing may not be the way to go. Due to the all the variables involved in degaussers and different types of data media IATRDD does not certify degaussing as a way destroying data.

When selecting a Technology Recycler to assist in your IT Asset Disposal process, be sure to select the one that will treat your data as a separate entity and destroy it accordingly. IATRDD recommends using an eGreen Certified Supplier that utilizes either physical destruction of the drives by shredding or uses DBAN (Darik's Boot and Nuke www.dban.org) to remove all data from the drives if the computers are going to be refurbished.

Bekah Alexandert
SVP/ General Manager
IAITAM