

When Destroying Data is a GOOD Thing!

At some point, all of us decide to “retire” our system(s) and acquire a new, faster replacement. Once you’ve migrated your files, settings and applications to the new system, you’ll probably make the decision to recycle it (there are a number of programs available now - including from the system vendors themselves) or pass it along to a charitable organization, school, friend or family member.

In any case, we believe that it is critical that you completely remove the private information, files and applications from system drives *before* you recycle or pass on your system - and that doesn’t mean placing files and information in the “recycle bin” and emptying it and uninstalling all of the applications. Why?

When you “delete” files and information or “uninstall” an application, the data isn’t really erased from your hard drive (or other drive type - floppy, Zip, etc.). That is why hardware or software-based data recovery tools from companies like:

- Acronis - Recovery Expert
- Executive Software - Undelete
- Final Data - Photo Retriever, FinalData Standard, Plus, Premium, FinaleMail
- iolo - Search and Recover
- McAfee - Easy Recovery
- OnTrack - EasyRecovery
- Symantec - Go Back, Ghost
- VCom - Recovery Commander

are all effective in finding and “bringing back” files that you accidentally deleted.

But what *you’ve* deleted and can recover using these tools, can also be recovered by unscrupulous individuals using the similar or even more powerful hardware and software. That’s why before you recycle or pass on your system - destroying data is a good thing! But how do you ensure your data/applications are erased - without trashing the hard drive?

There are a number of drive “wiping” applications available (amazingly enough from many of the same vendors that produce data recovery applications!) that can ensure secure deletion of any data on a hard drive or drive partition. These applications often offer wiping methods that range from the simple - overwrite the drive with a fixed value on every third sector to U.S. Department of Defense (DoD 5220.22-M) + Peter Gutman algorithm - overwrites the drive with a fixed value once, then its compliment value once then a random values once, the disk is then read to verify the overwrites, followed by overwriting the drive with random values four times on each sector, then overwriting the drive with chosen fixed values on each sector twenty-seven times and then writing random values four times on each sector (whew!). Your needs - and paranoia level - probably range somewhere in between these two extremes.

The table below outlines a number of “wiping” methods that vendors currently offer in their applications:

Method	What It Does	Level of Security
Zero Write	<p>Three possibilities:</p> <ul style="list-style-type: none"> • Overwrite with a fixed value (0x00) on every 3rd sector • Overwrite with a fixed value (0x00) on every other sector • Overwrite with a fixed value (0x00) throughout the entire area 	Low
Random Write	Overwrites with random values, often user selectable number of overwrite passes	Medium
Random and Zero Write	Combination of the two methods outlined above	Medium
U.S. Navy NAVSO P-5239-26-MFM	Writes fixed value (0xffffffff), then the fixed value (0xbfffffff), then random values. Drive is then read to verify overwriting process	Medium
U.S. Navy NAVSO P-5239-26-RLL	Writes fixed value (0xffffffff), then fixed value (0x27ffffff), then random values. Drive is then read to verify overwriting process	Medium
Bit Toggle	Overwrites drive four times, first with the value (0x00) then with (0xff), then (0x00), then (0xff)	Medium
Random Random Zero	Overwrites twice with random values then once with fixed value (0x00), then twice with random values and once with zeroes	Medium
U.S. Department of Defense DoD 5220.22-M	Overwrites by writing a fixed value, then its compliment value then random values. Drive is then read to verify overwriting process	Medium
U.S. Air Force AFSSI5020	Overwrites with fixed value (0x00), then fixed value (0xff), then a randomly selected constant. 10% of the drive is read to verify overwrite	Medium
North Atlantic Treaty Organization - NATO Standard	Overwrites seven times - first six overwrites are with fixed values (0x00) and (0xff) alternating between passes, 7 th overwrite is with random value	High
Peter Gutmann	Overwrites with random values four times on each sector then overwrites with fixed values on each sector twenty-seven times, then random values four times on each sector	High
U.S. Department of Defense DoD 5220.22-M + Peter Gutmann	Combination of the methods noted above	High

There are a number of software vendors marketing “wiping” software. They all offer one or more of the “wiping” methods outlined above as well as international standards such as Russian GOST and German VSITR. Make sure that the software you purchase supports the method you feel is the best for your needs and paranoia level (check out our Drive Utilities page for more information). Among the most popular are from:

- Acronis - Drive Cleanser (\$49.99)
- Broderbund - Complete Delete (\$19.99)
- Detto Technologies - Privacy Expert (\$29.99)
- East-tec - Shredder (free download), Eraser (\$9.95 per “wipe”), Format Secure (\$29.95), Eraser (Basic \$29.95, Standard \$39.95, Professional \$49.95)

- Iolo Technologies - Drive Scrubber (\$29.95, Professional \$89.95), System Shield (Personal \$39.95, Professional \$129.95)
- OnTrack - Data Eraser (\$29.95)
- VCom - Secure Erase (\$39.99).

We strongly recommend that you invest in one of these utilities (or one like them) to ensure that the system you recycle or pass-on doesn't come back to haunt you through an unscrupulous individual recovering and re-using your personal or business information!

February, 2005