

DATA DESTRUCTION STANDARDS



WE DO ITAD RIGHT

Lifespan

Beyond DoD

In the late 1990's, The U.S. Department of Defense (DoD) published specific standards to ensure secure data destruction from magnetic hard drives and magnetic tapes. A lot has changed since that initial standard was published.

LifeSpan has published many articles on the subject of secure data destruction, the original DoD "standard" and current technologies and standards. Our goal is to provide reliable information to IT organizations related to end of life data security and compliance. We have compiled three of our most referenced articles on the subject in this document to provide an overview of this important subject.



INCLUDED:

- 01 The DOD Standard: Useful or Obsolete?
- 02 Two Methods of Secure Data Destruction for Tapes
- 03 Should you ask for a "DoD" data wipe?

The DOD Standard: Useful or Obsolete?

Back in the 1990s, a standard for the destruction of sensitive data was created by the Department of Defense for hard drive and media being disposed of by the government's defense and security agencies. Coined the "DoD wipe", the process involved a 3-pass over-write procedure that would effectively erase data from a hard drive. At the time there were no other standards – government or industry – so most enterprises adopted this "DoD wipe" as their own policy. Even to this day, many companies will insist on this "DoD wipe" or "3-pass", despite it being obsolete as a government standard. The current reference standard is the NIST 800-88, Rev 1 document (which was updated in 2012 and adopted in 2014).

At the point of publication, the DoD wipe procedure made a lot of sense. But now there's little reason for the 3-pass wipe. Compared to 20 years ago, we have better hard drive technology and erasure software, and documented processes to ensure the erasure is successful.

Why a 3-pass Procedure Was Chosen

So why were three passes the magical number for erasure of data? Why not two or four or ten? Quite simply, it was thought that three was a good number. There was no testing that demonstrated three passes would be more effective than two or less effective than four. Based on the then-current hard drive technology, more than one pass was believed to be needed because of the precision of the write head and the way the firmware read and wrote to each sector. One pass might not get every sector overwritten, every time. A number was chosen that satisfied the needs of the Department of Defense.

Improvements in Drive Technology

When the DoD standard was adopted, technology was not nearly as advanced as it is now. In the 1990s, data sanitization practices were developed for slow magnetic hard drives with capacities less than 1 megabyte, and it was shown that a series of three manual passes would be sufficient. What

may confuse some non-IT professionals is why a single pass would now be as effective as three passes, based on the fact that hard drives have a much greater capacity. The reason for this is that two types of technology have advanced since the DoD standard was created. The first involves the technology of the hard drives that are in use. Today's drives are much more precise than older magnetic drives, which means that the head will write over every sector reliably with just one pass. The second improvement in technology comes from the software tools that have been created to assist in the procedure. Software tested and certified such as that from Tabernus or Blancco enable verifiable overwrites with detailed records.

Risk vs. Cost

It's a given that the less work that needs to be done, the lower the cost will be. A 3-pass procedure takes, you guessed it, three times as long as a single pass. This is significant with higher density drives. A 1Tb drive can take hours to fully wipe once (time varies depending on the drive interface, and the systems being used). Additional costs to do additional overwrite passes only increases processing costs and does not technically reduce risk.

Number of Passes vs Process

There is at least as much risk in the process for data destruction as there is in the technical erasure process. In this case, the process includes how you store, track and ship hard drives from the time you retire them until you dispose of them, what procedures your ITAD vendor has in place to ensure and document data destruction and also the quality assurance procedures.

Of course, if your company policy insists on 3-pass (or any number higher than 1) the software tools can be set to automatically perform the multiple passes and record the results. You should consult with a Data Destruction expert to determine the best options for your company. A NAID AAA certified company will have the expertise and the processes in place to ensure the security of your data.

Two Methods of Secure Data Destruction for Tapes

Does your company have volumes of backup tapes in your data center or offsite? If your company is at the end of a data retention period, or is ready to release or purge old archived data, you may come across hundreds or even thousands of tapes that contain important company data. Knowing what procedure is best to sanitize all of this data is crucial. There are two main options: physical destruction, and data destruction. One method may be better for you than the other depending on your company, the type of data, where it's stored, and how many tapes you need to securely sanitize.

LTO DLT Tapes for Data Destruction resized 600 Physical Destruction - Shredding

This is the 'brute force' option for data destruction. With this method, tapes are shredded, leaving the media unusable and scattered into small individual pieces that cannot be made whole again. With this method, the data on the tapes themselves remains intact. This usually won't matter, though, since reconstructing a shredded tape would be nearly impossible. It does make a mess, though. The volume of a tape increases by 4x after shredding.

Data Destruction - Degaussing

Degaussing is the only completely reliable way to sanitize data on magnetic storage media and is approved by the NSA and other major government agencies. The process eliminates the remnant magnetic field which holds the information on storage media such as tapes and hard drives.

Although degaussing leaves the media physically intact, the process will securely and completely sanitize the media and renders it useless when done correctly. LTO and DLT tapes contain a factory-written magnetic servo signal that is destroyed along with the data during the degaussing process.

One advantage of not physically destroying the media is that it is much easier to store and transport after the process is complete. A degaussed tape takes up the same amount of space it did before the data was destroyed, allowing the tapes to be transported or stored in containers. A good way to dispose of the degaussed tape is via an incinerator used for power generation. There are a number of these facilities around the country, though not in every state.

Know your degausser! Though handheld degaussers exist, they are slower and require a specific procedure to ensure full data destruction. They are also made for use on hard drives, and should not be used for degaussing tapes! Conveyor degaussers are able to wipe media in a continuous stream, and some are able to process nearly 2,000 tapes or hard drives per hour. Conveyors are also mobile, and the process can be performed inside of offices, data centers, storage locations, and more. All that is needed is a 120V power source and adequate space.

2014 Standards for Data Destruction Include Mobile Devices and SSDs

A lot can change in eight years, especially when we're talking about technology. Since the National Institute of Standards and Technology released NIST 800-88 in 2006, it has been the only official United States standard for data destruction, replacing the outdated DoD three-pass standard. But that was 2006, and data storage trends have evolved quite a bit since then. Most significantly, solid state drives (SSDs) and mobile devices like phones and tablets that make use of Flash SSDs have become ubiquitous in the workplace.

The most recent updates to the NIST 800-88 standard reflects the use of these devices and the need for a reliable process for destroying the data on them. If your company deals with sensitive information of any type, whether it's medical records, financial data, employee or customer personal data, or intellectual property, you need to be aware of these changes.

In late 2013, the first revision of NIST 800-88 was published. Although it is still technically a draft, it is the accepted industry standard for hard drive and media sanitization. What follows is an overview of some of the major revisions to NIST 800-88. It includes important new best practices for sanitizing both mobile devices and SSDs.

Sections 2.3 and 2.4

These sections deal directly with the standards for sanitizing solid state drives. As the cost of SSDs has declined, and their capabilities have expanded, an increasing number of businesses are using them for data storage. Unfortunately, as discussed in one of our recent white papers, the specifications of these devices make conventional magnetic data destruction strategies ineffective

These sections of NIST 800-88 address the inefficacy of overwrite technologies when applied to SSD devices, and the difficulty of destroying the drives completely due to the physical structure and the nature of the electronic storage. The new standards do not outline specific destruction standards, but they do recommend that SSD users be aware of their increased vulnerability.

Sections 4.7 and 4.8

Reviewing the practices of your own team or IT asset disposition (ITAD) vendor is a crucial but often overlooked part of the data destruction process. The destruction process must be documented so you can prove that data was destroyed properly. The newly updated sections reaffirm the necessity of an audit, and outline standards for the auditing process. Section 4.8 recommends that any audit should include details about:

- The device
- The process of destruction
- The method of destruction
- The date of destruction
- The name of the supervising party
- A validation of all of the above information

Without this document in your records, there is no guarantee that your devices were sanitized according to the best possible practices. The takeaway is that any ITAD vendor you select must be able to provide a comprehensive audit.

Appendix Updates

When the original NIST 800-88 data destruction standards were first drafted, smartphones were in their infancy. But as too many businesses have discovered, the capabilities of these devices are also a liability. The new standards include recommendations for sanitizing phones from all of the major providers, and they provide an important road map for true data security in 2014 and beyond. The appendix outlines the accepted method for data destruction at each level – clear, purge, and destroy. Notes addressing the unique challenges inherent to each device type are also included. If your business relies on a specific type of mobile, or a combination of devices, we absolutely recommend consulting the appendix.

The changes outlined in NIST 800-88 are important for all business, because the way data is stored in 2014 is not the same as it was in 2006 (especially concerning the rise in SSDs). For more information on Best Practices when it comes to erasing solid state disks, download this free whitepaper, “Advances in SSD Erasure Solutions.”

To learn more detailed information about the process of degaussing, request our degaussing technical brief and 10 Myths About ITAD Data Erasure. In both, you’ll learn more about NSA standards for degaussing and data destruction, Oersted’s and Coercivity, and why not all degaussers are created equal.

Contact us to request your copy today.

(888) 720-0900

itad@lifespantechnology.com

LifeSpanTechnology.com