blancco

How Many Times Must You Overwrite a Hard Disk for Complete Data Erasure?

Why Blancco

Blancco is the industry standard in data erasure and mobile device diagnostics software. Our data erasure software provides thousands of organizations the tools they need to enable sustainable data sanitization processes across the widest array of IT assets. By focusing on erasing and reusing assets instead of physically destroying them, organizations can improve their security posture and address corporate social responsibility requirements, while also ensuring compliance with local and global data privacy requirements.

Blancco data erasure solutions have been tested, certified, approved and recommended by 15+ governing bodies and leading organizations around the world. No other data erasure software can boast this level of compliance with the rigorous requirements set by government agencies, legal authorities and independent testing laboratories. All Blancco erasures are verified and certified, resulting in a tamper-proof audit trail.

The safest and most cost-effective way to make data disappear without having to destroy a hard disk drive (HDD) is to simply overwrite it. But how many overwriting passes are sufficient? Or, as some put it, how many times do you write ones, zeroes, or other junk data to a hard drive before confidently telling customers their data has been completely wiped?

It may be fewer than you think.

First, let's take a look at the target of all these concerns: the hard disk drive—also referred to as a "hard drive" or "hard disk"—and what it means to overwrite one.

Earlier Approaches to HDD Data Removal

The process of removing data from storage media has been examined by different government agencies and organizations many times during the past 20 years. In the U.S., 3- and 7-pass methods were once advocated by the Department of Defense, beginning in the mid-1990s. Across the Atlantic, other organizations also advocated multiple passes. In the early 2000s, the VSITR standard by the German information security agency, BSI, applied seven overwriting passes. It soon became popular in Europe to use overwriting standards that consisted of four to seven passes. Other approaches recommended even more.

However, in 2006, the DoD 5220.22-M operating manual (PDF) removed mention of any overwriting requirements. Instead, it delegated that decision to government oversight agencies (CSAs, or Cognizant Security Agencies), allowing those agencies to determine best practices for data sanitization in most cases.

Meanwhile, also in 2006, the U.S. National Institute of Standards and Technology (NIST) released its "Guidelines for Media Sanitization (PDF)." These guidelines stated that "for ATA disk drives manufactured after 2001 (over 15 GB) clearing by overwriting the media once is adequate to protect the media."

> "
>
> For storage devices containing magnetic media, a single overwrite pass with a fixed pattern such as binary zeros typically hinders recovery of data even if state of the art laboratory techniques are applied to attempt to retrieve the data."
>
> -NIST SP 800-88, Rev. 1, "Guidelines for Media Sanitization," U.S. National Institute of Standards and Technology

NIST 800-88, BSI and NCSC Allow a Single Overwriting Pass

When NIST revised its guidelines in late 2014, it reaffirmed that stance. NIST 800-88, Rev. 1 (PDF) states, "For storage devices containing magnetic media, a single overwrite pass with a fixed pattern such as binary zeros typically hinders recovery of data even if state of the art laboratory techniques are applied to attempt to retrieve the data." It noted, however, that hidden areas of the drive should also be addressed.

For ATA hard disk drives and SCSI hard disk drives specifically, NIST states, "The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used."

Even for Purge, one pass will suffice, it said, though an inverted three-pass method is also an option.

NIST's guidelines have become a global reference document with principles incorporated into notable international standards such as ISO/IEC 27040:2015 and various countries' data destruction best practices or requirements.

Today, internal operating manuals based on NIST 800-88, Rev 1. "Media Sanitization Guidelines" (see our blog on NIST) usually specify two kinds of procedures:

- **clearing** (to prevent recovering data using software) and
- **purging** (to prevent recovering data using laboratory techniques).

Clear procedures generally involve overwriting the HDD. Purge procedures with higher security requirements can vary but usually involve overwriting techniques combined with the execution of internal HDD commands (firmware-based erasure). (NOTE: Degaussing (demagnetizing) or physical destruction of media renders the media unusable, but even then, can sometimes leave recoverable data behind).

This software-based method securely overwrites data from any data storage device by writing zeros and ones onto all sectors of the device. By overwriting the data on the storage device, the data is rendered unrecoverable and achieves data sanitization. The data sanitization process involves a complete removal of data, as well as verifying and certifying that erasure has been performed successfully.

The nature of the data (how confidential it is) as well as other considerations (whether the hard drive is leaving the customer's organization, for example) determines whether Clear or Purge are most appropriate.

Other governments have decreased their overwriting numbers similarly: the HMG Infosec Standard 5, published by the British CESG (now part of National Cyber Security Centre), currently defines two approaches: one with one overwriting pass and one with three overwriting passes. In 2012, the newer BSI GS standards were made public, combining one to two overwriting passes of random data with firmware-based erasure.

However, keep in mind that the overwriting techniques discussed thus far are intended for magnetic hard disk drives, not flash-based SSDs.

A Note on SSDs—and the Challenge of Erasing Them

With the rise of laptops and the need for speed, non-volatile storage trends have seen an uptick in solid-state drives (also known as flash memory drives or SSDs). And though the technology has been around for decades, it wasn't until 2005 that Samsung declared SSD as a strategic market.

Today, SSDs come in different interfaces/technologies (SATA, SCSI/SAS, eMMC, Fusion-io, NVMe/PCIe, USB) and form-factors (2.5-inch, mSATA, M.2, AiC PCIe). Faster, more reliable, and allowing for more storage capacity than their HDD counterparts, SSDs are highly efficient. They are also smaller, lighter, more resistant to damage and consume less power.

However, they also come with data destruction concerns: SSDs are difficult to physically destroy to an acceptable level, and methods like degaussing don't work on them. While NIST allows minimum one-pass overwriting for SSDs, it's almost always combined with specialized commands, technologies, or tools and with additional steps required to reach all sectors. This is because SSDs have mechanisms that minimize wear (wear leveling) by using non-addressable overprovisioning areas within the drive where data can be left behind. Furthermore, multiple passes also come at a cost: premature wear on SSDs that reduces the overall lifetime of the media.

Fortunately, Blancco not only erases magnetic-based hard disk drives, we also offer a patented SSD erasure method to fully and securely overwrite different types of SSDs, simplifying the process and speeding up erasure across a range of flash-based storage devices.

> "
>
> **In the end the final decision on which erasure standard to use, and therefore, the number of times to overwrite your drives, rests with the customer's specifications and requirements.**
>
> **As the global leader in certified data erasure, Blancco supports 25+ international erasure standards set by government agencies, legal authorities, and independent testing laboratories.**

Conclusion: One Overwriting Pass is Sufficient for Erasing HDDs

The technology changes in the last 15 years, such as the ever-increasing data density on disk platters, have made all attempts to recover data after overwriting unlikely. Multiple overwriting passes for hard disk drives is not an absolute necessity anymore.

One pass is enough.

However, to ensure the overwriting process has been effective, major agencies and government bodies worldwide (NIST, NCSC, BSI and others) require a specific step: verification of data erasure is mandatory for full compliance with their standards.

To summarize, securely overwriting hard disk drives involves:

- **One overwriting pass for most HDD erasure.** Remember to weigh data sensitivity against the costs of a higher level of security and the time you want to spend on each processed asset. More passes take longer and are usually unnecessary.
- **Utilizing the drive's firmware-based erasure commands,** when available, as a valuable addition, particularly when erasing sensitive data.
- **Removing and erasing any hidden areas on the HDD** as part of the erasure process in those cases.
- **Remembering that what works for HDDs does not apply to flash-based storage (SSDs):** match your erasure method to your media type.
- **Verifying erasure,** whether at the end of the process or after each overwriting round to ensure that data sanitization has occurred and to comply with most data erasure standards.
- **Documenting erasure:** The best erasure is the one you can prove; therefore, a report documenting verification and certification of the erasure of a media support is also necessary.

Overwrite Your Data Storage Drives with Our Free Data Erasure Trial

In the end, however, the final decision on which erasure standard to use, and therefore, the number of times to overwrite your drives, rests with the customer's specifications and requirements.

As the global leader in certified data erasure, Blancco supports 25+ international erasure standards set by government agencies, legal authorities, and independent testing laboratories.   Blancco Drive Eraser software has been designed to support the widest variety of HDDs and SSDs in both PCs and laptops   (including Mac T2 devices) and servers.

> Choose from one pass to as many as you require—and be confident that Blancco solutions erase data completely and permanently from all your drives.