Erasing Devices With NIST 800.88r1 Overwrite Pattern

WHITE CANYON™
SOFTWARE

www.WhiteCanyon.com | Sales@WhiteCanyon.com | 1 (801) 224-8900

Implementation and Erasure with the NIST 800.88r1 Overwrite Pattern.

As stated in the NIST 800:88r1 “The modern storage environment is rapidly evolving.” This constant and sometime drastic changes is causing major data management issues unless organizations properly align their policies with current guidelines.

The evolution of storage equipment has also caused an increased concern for data breaches. This has elevated the interest in secure methods for wiping electronic device information. When a device reaches the “end of its life”, a company can no longer carelessly toss it aside.

The traditional “format the hard drive” approach does not meet standards. Hackers are still able to reach 90% of data on these devices. Thus, more sophisticated tools are now available to create a total eradication of data. These premium tools provide secure services and functions. They also generate reports for IT departments that certify the data wipe.

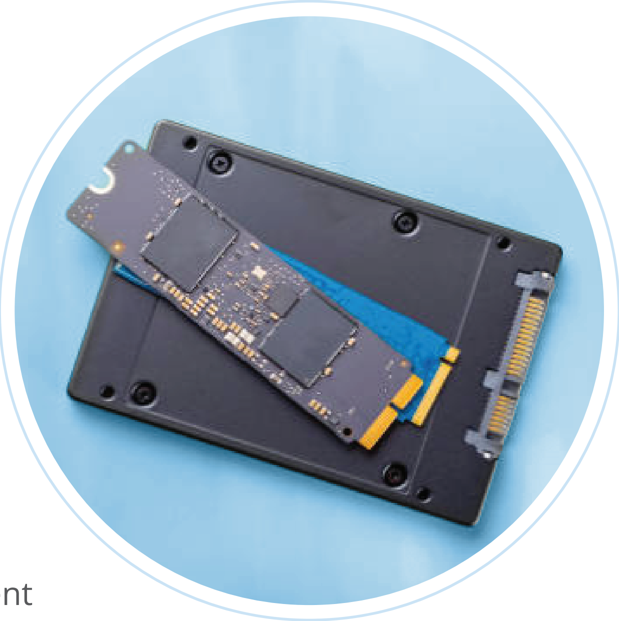
Effective data wipes remove all information. This includes sensitive information that a company would not want carelessly released, when considering selling or recycling older devices. Additionally, it will remove any malware infections, pirated software, or Trojan horse files that may be on the device, giving the company confidence it is reallocating clean hardware.

This article discusses the new developments in storage technology and the new requirements these devices require to be securely erased.

National Institute of Standards and Technology

The National Institute for Standards and Technology (NIST) is an organization that creates commercial standards for materials and products. NIST standards are common in many industries and NIST first released standards to address the sanitization of data on media devices in 2006. The most recent release in 2012, (NIST 800-88r1) provided methodology to address SSDs and other types of storage devices, mainly ATA commands and it provided further recommendations for data wiping.

NVME VS. SSDS



Data storage has evolved into two new types of drives; the non-volatile memory express (NVMe) and the solid-state (SSDs). NVMes offer quicker data transfer between drives and computers. Their architecture includes a host controller interface with a storage protocol to accomplish transfers faster than traditional drives.

The SSDs offer quick boot up times and fast loading of programs, files, and systems. These types of drives have become popular in personal computers and are used extensively in the datacenter environment.

The SSD, NVMe and HDD are not the end of development for storage devices. Work is currently being finished on HAMR and EAMR drives and there will be new storage breakthroughs in the future.

These new types of drives need to be addressed by wiping standards.

HOW TO WIPE THE DATA

There are still people who believe that multiple overwrites will remove the bit shadows and overlays on hard disks. With modern high-density disks, this approach is no longer necessary. The precision of new hard drives and where they write the 1's and 0's removes the risk of electromagnetic recovery. Multiple overwrite passes are no longer necessary. Hard drives can now be securely erased with a single overwrite pass.

SSDs and NVMe drives require different protocols to reach secure erasure. The data on these types of drives are stored in memory chips and there are more chips on the drive than labelled on the devices. The Advanced Technology Attachment (ATA) compliant drives have a drive controller built into the drive itself. Companies and products now send commands to the SSDs to overwrite the drive. They can also wipe SSDs that are not ATA compliant. Today, you can wipe modern disks, NVMes, and SSDs with a single overwrite using null bytes.

The multiple pass overwriting on SSDs, NVMe and HDDs is pointless and decreases the service life of the device.

COMPARISON TO THE DOD WIPE STANDARD

There are many companies that use the Department of Defense (DOD) Standard. This isn't actually a standard. It is a reference to the National Industrial Security Program Operating Manual (NISPOM).

This manual addresses all areas of government-industrial security. One article describes the method for wiping drives. The initial DOD wipe sanitization standards were delegated to "Cognizant Security Authorities". At one time, the Defense Security Service recommended a 3- or 7-pass wipe for clearing drive data. Thus, this is where we get the DoD3 and DoD7 overwrite patterns. These overwrite patterns included which character to use in the overwrite pass and the number of verifies.

In 2006, the U.S. Department of Commerce convened the National Institute of Standards and Technology (NIST). NIST serves as a non-regulatory agency in the Department of Commerce. NIST updated the requirements for data erasure when they published the NIST Special Publication 800-88. This was later revised in December 2014. The current standard that companies should follow is the NIST SP 800-88 Rev 2.

HOW DOES THE NIST STANDARD ADDRESS DATA

The NIST SP 800-88 Rev.2 states the following definition for disk sanitization:

"The general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed."

The NIST Framework for Improving Critical Infrastructure Cybersecurity sets forth the security activity levels. The highest cybersecurity levels, known as functions, are as follows:

- Identify
- Detect
- Recovery
- Protect
- Respond

You will want to assess your data and assign a level of confidentiality. Examine all types of media used in your business and determine each item's risk level for exposure. Companies use these levels to manage their cybersecurity risk. This helps organize information, facilitates risk management decisions, and addresses possible threats or other issues.

Today, data moves through many different companies, systems, and storage devices. This increases the difficulty in controlling the propagation and tracking of data. Also, many data storage systems now rely on a distributed cloud-based architecture.

The originating company and all users who store data are responsible for data wipes. Using encryption and sophisticated access controls decreases the risk of breaches. But, hackers have turned to discarded devices to obtain residual data. The data on these sold, donated, or reallocated drives should be completely wiped before releasing devices. It is important to scrutinize all internal equipment before transferring to another source or entity.

NIST CATEGORIES FOR SANITIZATION

The NIST SP 800-88 Rev 2 groups sanitization into three categories:

- **Clear the Data**

  This method uses logical strategies to wipe data. This includes all user-addressable storage locations and protects against non-invasive, simple data retrieval attempts.

  The standard Read and Write commands is usually the interface used in this technique, as the user rewrites new data over the old data or resets the device to its factory settings.

- **Purge the Data**

  Sometimes you will hear the terms clear and purge used interchangeably. Purging uses physical or logical strategies to make the target data unrecoverable. This often involves the use of state-of-the-art laboratory methods and has a much higher tolerance than Clear.

- **Destroy the Data**

  The destroy technique involves the destruction of the media storage device. This ensures that none of the data is subject to retrieval. Also, no one will have the ability to use the media in the future. However, this method is not eco-friendly considering you are destroying hardware that could still be used.

The clear and purge of data is the responsibility of data erasure software tool. This is performed on the different media storage available in an organization. The following section discusses how to address these devices.

MAGNETIC MEDIA STORAGE DEVICES

One standard method for magnetic media involves a single overwrite pass using fixed patterns such as binary zeros. Even state-of-the-art techniques cannot retrieve data following this type of sanitization. Yet, this is not without limitations.

Data erasure tools that only use the Read and Write interface may not address all areas of the drive. Data erasure software should use other interfaces to address areas that are not actively mapped to the Logical Block Addressing (LBA). This could also include defect areas, remapped sectors, DCO areas, HPA and unallocated space.

Using overwrite protocols and old techniques with evolving media types increases the risk of data breaches. While the host interface is the same or nearly the same, the underlying media may change. It is vital to match the sanitization technique to the current media.

CRYPTOGRAPHIC ERASURE (CE)

One of the newer sanitization techniques addresses encrypted data on storage media. CE wipes the cryptographic keys used for encrypting the data. This eliminates the possibility of recovering the data without the encryption key.

The CE approach is often quick and supports partial or selective sanitization. This is accomplished by focusing on a specific storage media subset. The technique has possible use in cloud computing and with mobile devices.

Sometimes, it is difficult to verify the data wipe using CE. We recommend using CE along with other verifiable sanitization methods for best results.

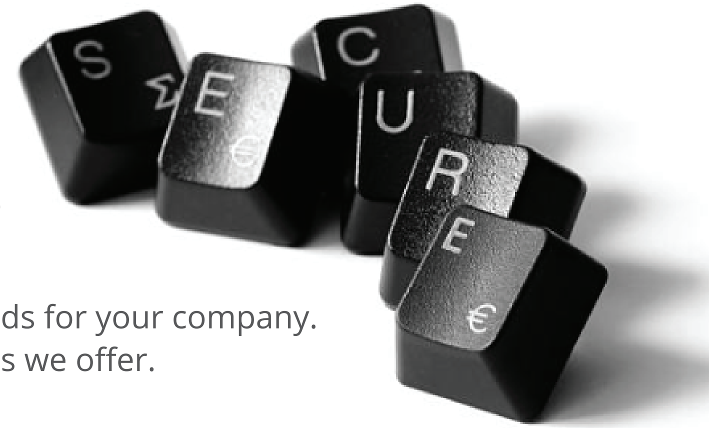
OTHER CONCERNS REGARDING SANITIZATION

Several avenues remain that can place you at risk for data breaches. Many of these are often overlooked. For example, monitor screens may have data burned into the screen. Other storage media, such as removable devices, can become misplaced, forgotten, or lost.

NIST COMPLIANT DATA SECURITY

As a business owner or IT manager, it’s hard to keep up with the ever-changing technology and regulations. Hackers continue to target new vulnerabilities. Thus, companies must constantly improve procedures to protect company and customer data.

This article describes the previous DoD Wipe Standard and the NIST R2 standards. Every type of device that stores, uses, or sends protected or classified data must meet these standards. Likewise, repurposed, reassigned, or decommissioned hardware must undergo data sanitization.



WipeDrive Enterprise can meet these data security needs for your company. Request a trial today and discover the security solutions we offer.