Technology Paper

Media Sanitization Practices During Product Return Process Best Practices Statement

Objective

This statement provides Seagate customers with an overview of what happens to data on products when returned to Seagate. In order to protect your privacy and other interests in data, you should delete all data, or as much as possible, prior to returning any product to Seagate. Seagate realizes, however, that you may not be able to erase certain data on returned products. In any event, Seagate will take the steps described in this statement to protect the physical security of such products and, if applicable, overwrite data as early as possible on products recertified by Seagate.

Seagate has coordinated with the National Security Agency (NSA) and the Center for Magnetic Recording Research (CMRR) to ensure that any products repaired by Seagate are in compliance with or exceed the appropriate U.S. Government specifications. The National Institute of Standards and Technology (NIST) provides certain standards regarding drive sanitation. The relevant specification, contained in the September 2006 Special Publication 800-88, *Guidelines for Media Sanitization*, defines that an accepted drive sanitation for magnetic media is a Purging of data on the media.

Media Sanitization Practices During Product Return Process Best Practices Statement

NIST 800-88

NIST publication 800-88, section 2.4, table 2-1, Purging: "Purging information is a media sanitization process that protects the confidentiality of information against a laboratory attack. For some media, clearing media would not suffice for purging. However, for ATA disk drives manufactured after 2001 (over 15 GB) the terms "clearing" and "purging" have converged.

A laboratory attack would involve the threat with the resources and knowledge to use nonstandard systems to conduct data recovery attempts on media outside their normal operating environment. This type of attack involves signal processing equipment and specially trained personnel.

Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging."

ATA Secure Erase

The AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS) document defines the command SECURITY ERASE UNIT: "When Normal Erase mode is specified, the SECURITY ERASE UNIT command shall write binary zeroes to all user data areas (as determined by READ NATIVE MAX or READ NATIVE MAX EXT)." "When Enhanced Erase mode is specified, the device shall write predetermined data patterns to all user data areas. In Enhanced Erase mode, all previously written user data shall be overwritten, including sectors that are no longer in use due to reallocation."

The ATA Security Erase command, once initiated, runs entirely within the drive and reports busy until the command (full erasure) is complete.

Seagate has verified that not only does its repair process overwrite user addressable locations, but the process also overwrites the non-user accessible locations. Seagate uses random characters, high-frequency patterns and digital zeros patterns to match the drive design technologies.

What is the Product Return Process?

Seagate maintains several collection depots throughout the world for the purpose of receiving warranty returned product. These sites are highly automated and optimized to screen the returned products into two fundamental groups. A significant percentage of drives returned to Seagate are determined to have No Trouble Found (NTF). These drives are separated from the rest for a faster recertification process. The rest of the drives are shipped back to Seagate factories for evaluation and repair.

In the case of SATA interface NTF drives, Seagate uses the ATA SECURITY ERASE UNIT command, Enhanced Mode, as recommended by NIST 800-88. After media sanitization, the drives are relabeled

and marked as Certified Repaired HDD drives.

In the case of drives returned to the factory, these drives are "re-processed". When disk drives are manufactured, after the physical assembly of parts, the drives are "processed". This is where the drive is given its initial low level format, servo calibrations and media defects assessment and reallocation. New drives are fundamentally blank with regards to data. Re-processed drives are also blank in the same way. Re-processing drives has the effect of full media sanitization and exceeds the ATA SECURITY ERASE UNIT command in thoroughness and coverage.

All Seagate recertified drives have a unique top cover label with a green border to distinguish them from newly built products. Both NTF and re-processed drives are given the same unique label.

Media Destruction on Failed Drives

Drives that are deemed not repairable or have no repair demand are scrapped and recycled for their metals. The scrapping procedure begins with physical destruction of the entire hard disk assembly which completely destroys the media. Destruction of media is the ultimate form of sanitization. These activities are carried out effectively and securely prior to sending for raw material reclamation.

Seagate Self-Encrypting Drives (SED)

Many Seagate 2.5" drives are available with a self-encrypting capability. All data written to the media is AES-128 encrypted using a unique encryption key. No two drives have the same key, so no two SED drives write the same data patterns to the media when given the same data to write. For SED drives, the SECURITY ERASE Enhanced command causes the SED encryption key to change, thus instantly rendering useless and gibberish any previous data on the device. This includes any reallocated sectors and should conform to NIST 800-88. Some Seagate SED drives have the further distinction of having NSA FIPS-140-2 certification. Seagate SED drives are always re-processed.

Non-SATA Interfaces SAS, SCSI and Fibre Channel

An internal secure erase command is defined by the ANSI SCSI specifications. It is called "Security Initialize" and is functionally equivalent to the ANSI ATA specification.

USB External Drives

USB drives have a SATA drive contained within them. A small circuit board bridges and joins the SATA and USB interfaces. Some USB bridge cards restrict the ATA SECURITY ERASE command, while others allow it. Newer Seagate USB products are given full media sanitization using the ATA

SECURITY ERASE. Products that do not allow the command are given a full pack block overwrite of the media with zeros. Since Seagate USB products are built to full native maximum capacity, this full pack block overwrite is functionally equivalent to SECURITY ERASE in normal mode and therefore should conform to NIST 800-88 purging guidelines.

Other Seagate Utility Software (block overwrite) NIST 800-88 Clearing

The less secure level below NIST 800-88 Purging is call Clearing. Clearing also overwrites all sectors on a drive as it is defined by the interface capacity commands. In other words, a drive may be defined smaller, which causes the blocks above the new size to become unknown to software-based block overwrite utilities. While rare, a size-adjusted drive hiding blocks is why clearing and purging media sanitization are different under NIST 800-88. Another difference between the two is the way the media sanitization activity runs. Clearing is managed block-by-block in the software; you can see it count up through the blocks and the software usually displays a progress bar. This type of control is subject to interception by malicious software. Purging software is a single command that puts the drive offline from the interface and it just runs and is busy until it finishes.

Seagate *SeaTools* utility software with block level clearing media sanitization is available from the Seagate website at www.seagate.com/support/seatools Seagate is not responsible for lost user data.

Summary

If data security is important to you while a returned drive is in transit to Seagate, then you should consider clearing the drive's data before sending it. Your shipping service may provide delivery verifications which may be important to you considering the previous data on the drive. Once a product has been returned to Seagate, we protect the physical security of the drive. Furthermore, we perform best-practice media sanitization as early as possible to remove the data that was brought with the device.

AMERICAS Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
ASIA/PACIFIC Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 16–18 rue du Dôme, 92100 Boulogne-Billancourt, France, 33 1-4186 10 00