Phiston TECHNOLOGIES® INC.
Innovation, Ingenuity, Integrity

How to Destroy SSD Drives (And Does Degaussing Work on Them?)

Formatting an SSD drive is not enough to make the information stored in it irretrievable. Here's what you need to do to properly dispose of it.

ABSTRACT

Due to how these devices store information, safely disposing of an SSD drive is not as easy as you might expect. So, if you're considering donating or formatting your solid-state drives, there are several considerations you should keep in mind to ensure the data stored in them is made truly irrecoverable.

Simply deleting files is insufficient to remove all the data from an SSD. In fact, if you are storing sensitive information, you might have to use physical destruction (like shredding or incineration) to guarantee it never falls into the wrong hands.

In this article, we will go through everything you need to know about how SSDs store data and how you can get it properly destroyed.

HOW DOES AN SSD DRIVE WORK, AND WHY DOES IT MATTER FOR DATA DESTRUCTION?

Solid state drives work in quite a specific way. Something that is important to keep in mind is that they use NAND-based flash memory chips to store and retrieve data (they require no power to do so). So, unlike traditional hard disk drives (HDD), which use spinning disks to read and write data, SSDs have no moving parts.

Each cell in a NAND-based flash memory chip has a specific amount of storage capacity, which can be either "on" or "off" depending on whether an electrical charge is present or not. To read data from the SSD, the controller in the drive sends electrical signals to the cells to determine the presence or absence of a charge and then interprets this data to retrieve the stored information.

Because of this, SSDs are generally faster, more durable, and more power-efficient than HDDs.
When it comes to data destruction, though, SSDs can pose a unique challenge compared to HDDs. Because of the way that data is stored on SSDs, simply overwriting the data with new information may not be enough to completely erase the original information. This is because the SSD controller may move data around within the flash memory chips to optimize performance and prolong the life of the drive.

DELETING DATA STORED IN SSDS

To ensure complete data destruction on an SSD, you will need specialized software or hardware that can overwrite the entire drive with random data multiple times, something that can effectively erase any remaining traces of the original information and make it unrecoverable.

Alternatively, you can encrypt the data on the SSD (and lose the encryption key, so to speak). If you then format the drive, then it would be very unlikely for anyone to be able to break the encryption and recover the information.

Neither of these methods is entirely foolproof, so there is always a chance some of the data will remain accessible.

CAN YOU DEGAUSS AN SSD?

Unfortunately, although degaussing is an effective data destruction method for HDDs and other magnetic media (like floppy disks, cassette tapes, etc.), it will not work on SSDs.

The reason is that degaussing uses a strong magnetic field to do this, and SSDs use flash memories (that do not store data magnetically). So, exposing a solid-state drive to a degausser will not erase the information - and might, in fact, damage the drive and render it unusable instead.

IS THERE A WAY TO GUARANTEE DESTROYING DATA WILL WORK?

If you want to ensure your sensitive data is made completely irrecoverable, the best solution is to physically destroy your SSD using a technique like shredding or incineration.

If you are storing data that is particularly sensitive (for example, healthcare information or customer information regulated by compliance and sanitization requirements), you should consider using specialized equipment and expertise.

DIFFERENT WAYS TO DESTROY SSDS

There are three main methods for destroying data stored on SSDs: Shredding, incinerating, or using a (dangerous and not-recommended) acid bath. Let's go through each of these destruction methods in some more detail.

SHREDDING SSDS

Shredding is a method of physically destroying an SSD by reducing it to tiny pieces using a specialized shredder. This method is often used for the large-scale destruction of electronic devices and ensures that the data on the SSD is completely destroyed beyond any hope of recovery.

A shredding machine will provide certain users with a good level of assurance that the data is destroyed. However, some companies require a higher security level (for instance, those working with the government or security agencies). In this case, shredding will need to be done in a specific way; typically, transporting the SSD to a dedicated shredding facility.

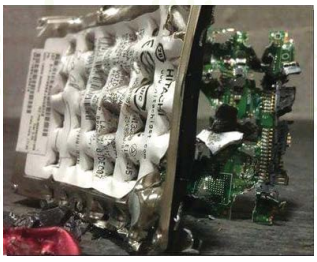
INCINERATING SSDS

Incineration involves burning the SSD at high temperatures until it is completely destroyed. This method is often used for sensitive or classified data that must be made absolutely irretrievable to prevent unauthorized access.

Again, this must be done in a specific manner. Some commercial incinerators have cold spots inside, so using them to destroy an SSD might result in some surfaces being protected from the heat (usually by their casing). So, in order for incineration to work on SSDs, it needs to be done in a furnace capable of reaching 2000°C throughout. As with the previous method, incineration should only be carried out by trained professionals who have the appropriate equipment and safety protocols in place. It also needs to be done in compliance with local laws and regulations regarding the disposal of electronic waste.

OTHER METHODS OF DESTROYING SSDS

There is one more method for destroying SSDs, although it is considered highly dangerous, as it involves using hazardous materials. We're talking about acid baths, which submerge the drives into a corrosive acid solution that dissolves its materials and components, destroying the data in the process. We do not recommend this method.



CONCLUSIONS: HOW TO SAFELY DESTROY SSD DATA

SSDs pose a unique challenge regarding data destruction because they store data in flash chips and not magnetic media like HDDs do.

To completely and permanently delete the data stored in a solid-state drive, the best option is to destroy the drive itself physically. You can do this by using shredders or incinerators.

It's important to note that all the destruction techniques we have mentioned in this article should only be used by trained professionals who have the appropriate equipment and safety protocols in place. Additionally, it's essential to ensure you are complying with electronic waste disposal rules.

At Phiston Technologies, we are leaders in data destruction products. We have been making innovative and competitive destruction machines since 2009 and will be able to help dispose of your SSDs safely and in compliance with the strictest regulations. Contact us today to find out more about our products (which include destroyers, disintegrators, and degaussers) and how we can help your business.

THE PHISTON ADVANTAGE

At Phiston Technologies, we believe in innovation, proactive product development, and secure destruction of data.

Our goal is simple: destroying your media to preserve and promote data security. We build products to ensure complete media destruction.

As data storage continues to evolve, so will the need to advance current data destruction products. Phiston will always be ready to provide security solutions to keep your organization safe and in compliance.

Phiston as a company is a leader in end-of-cycle media destruction and has various products that can handle all. Our clients include some of the largest tech companies in the world, and our devices are deployed across all 50 states and in 49 different countries.