Phiston TECHNOLOGIES® INC.
Innovation, Ingenuity, Integrity

Best Practices for Data Destruction

Data destruction aims to completely erase all electronic data in a hard drive or storage media. A guide to all best practices and disposal methods.

ABSTRACT

Data destruction, or data erasure, is a way of overwriting data to entirely wipe the contents of a hard disc or digital media. Most data protection standards require businesses and organizations to confirm the information is truly gone so it cannot be used for unauthorized purposes. This is why many companies rely on a data destruction service to ensure the work is done correctly.

So, what are the best practices for data destruction, and how is it different from data sanitation? In this article, we'll go through everything you need to know about the current regulations, recommendations, and all the available destruction and disposal methods.

WHAT IS DATA DESTRUCTION, AND WHY DOES IT MATTER?

The purpose of the data destruction process is to make the stored data (usually sensitive data) no longer accessible. Deleting files is not enough. For data destruction to be effective, the software needs to also overwrite the blocks or spaces with random information to make it irretrievable by the original application or operating system that created it.

There are other ways to destroy that that don't depend on software. For instance, degaussing (a demagnetizing process that delivers a powerful magnetic pulse and sanitizes the data in seconds) or by using mechanical means to physically destroy data stored in drives (like drive shredders, disintegrators, and melters). Many data destruction companies specialize in these destruction services and more.

The Difference Between Data Destruction and Data Sanitization

Oftentimes, the term data destruction is used interchangeably with data sanitization. However, these are different methods with different requirements.

Data destruction makes data stored in hard disks, tapes, and other forms of electronic media unreadable. If you want to confirm the information is truly gone and cannot be accessed, you must comply with additional protection standards or ensure data sanitization. So, unlike data sanitization, hard drive data destruction does not include verification.

Let's see an example. Suppose you need to remove individual files from a hard drive. Many secure data destruction methods will not remove the files themselves but rather the pointers to them. This means that the information is still on the hard drive, even though the operating system cannot see it. Even file shredding or a full reformat can leave data behind, and there are ways in which it can be made accessible again. For instance, using forensic tools and keyboard methods.

How much of the data will remain depends on the destruction method and the type of media, but the most important takeaway from this distinction is that data destruction doesn't always protect you against industry regulations and requirements. Let's see why.

Data Destruction and Compliance Problems

Data destruction standards have been increasingly gaining prominence in several sectors and industries. Their goal is to help organizations and companies attain compliance. For example:

- **Secure data destruction in the healthcare industry:** In order to safeguard the privacy of protected health information, several acts (such as HIPAA in the United States) make it mandatory for entities and associates to protect health-related patient data. In particular, they give instructions on how to dispose of certain sensitive information, such as diagnosis and treatments, security numbers, and driver's license numbers.

- **Secure data destruction in the banking and finance industry:** Several regulations and standards also mandate organizations and institutions to destroy data in accordance with them. Examples of them include the Fair and Accurate Credit Transaction Act (FACTA) Disposal Rule, the Payment Card Industry Data Security Standard (PCI-DSS), the Gramm-Leach-Bliley Act (GLBA), the Bank Secrecy Act, and the Sarbanes-Oxley Act (SOX), among others.

- **Secure data destruction in defense services:** Several defense and security services also have specialized data destruction standards. The United States Army, Air Force, Navy, and the NSA have had these in place for dozens of years (there is, in fact, a list of NSA-listed techniques you can use to deal with the disposing of data). Earlier examples include US DoD 5220.22M, NSA 130-1, and Air Force System Security Instruction 5020, while there are also newer guidelines such as NIST SP 800-88.

Due to the prevalence of electronic data (and the advent of solid-state drives or SSDs and hybrid drives), new guidelines have emerged that are designed to standardize physical and logical data destruction and ensure secure data disposal.

For instance, NIST SP 800:88 was first published in 2006. This group of sanitization guidelines defines three methods for attaining data destruction for magnetic, optical, flash, and span media and devices: Clear, Purge, and Destroy. These work as follows:

- **NIST Clear:** This overwriting method uses standard Read/Write commands to rewrite the data in all user-addressable memory locations and give it a new value to protect it against non-invasive data recovery techniques.

- **NIST Purge:** This method combines overwriting, cryptographic erase, and block erase to use specific commands capable of destroying data. For example, you can use the block erasure technique to sanitize solid-state drives (by using special commands that increase the voltage levels in memory blocks and drop them to zero suddenly to delete all data). Or you can use cryptographic erasure to wipe a self-encrypting drives' Media Encryption Key (or MEK) and make the data unreadable if you don't have the encryption key.

- **NIST Destroy:** Lastly, this method combines different techniques, such as disintegration, shredding, incineration, and melting, to physically destroy data (and the devices where that data is stored).

Depending on the storage media, you will use a different set of guidelines. For example, paper and microforms can be shredded using cross-cut shredders (NIST Destroy), routers and switches can be reset to factory settings (NIST Clear) or disintegrated (NIST Destroy), and magnetic disks can be overwritten and verified (NIST Clear), degaussed (NIST Purge), or incinerated (NIST Destroy).

So, How Does Data Destruction Differ From Physical Destruction?

We've gone through different methods for destroying data, some of which include physical destruction. Of course, these two things are not the same.

Physical destruction refers specifically to the process of rendering a device (such as a hard drive, a tape, or a flash card) completely unusable. This is typically done by breaking the device or component into tiny pieces (sometimes as small as 2 mm). In some cases, physical destruction is also covered by the degaussing process, which uses strong magnets to destroy data instantly in seconds.

Just because a hard drive has been physically destroyed, it doesn't mean the information stored in it is gone. This is especially the case when talking about SSDs, which store information so densely that some shredded bits can still keep it intact. Even when degaussing HDDs, it's important to follow the correct procedures to guarantee secure data disposal. For example, the magnetic force of the machine needs to be strong enough to handle the hard drive, or some of the data might remain unaffected.

DATA DESTRUCTION BEST PRACTICES

No matter if your industry requires you to comply with certain guidelines, having good data destruction practices in place can help you protect your electronic devices from data breaches. Let's now go through some good practices and tips to overcome common data security challenges.

1. Establish a Records Retention Schedule (and Stick to It)

A records retention schedule is a policy document that identifies for how long you are supposed to retain data for operational and legal purposes. This document establishes how long important information must remain accessible for future use or reference and also provides disposal guidelines for how these items must be discarded (this also provides legally defensible processes).

Typically, there will be different schedules depending on the type of data and the ownership. By establishing one, you will be able to, first of all, promote consistency. Records of the same type will always be retained for the same amount of time, making the entire process more efficient, too. After all, you don't want to spend staff time, equipment, and space retaining records unnecessarily.

Many companies know they need to keep records for a long time in order to comply with freedom of information acts and legislation. In fact, it can be a personal criminal offense to destroy data requested through these acts. If you have a records retention schedule, you will also have accountability and be able to demonstrate you have taken measures to follow proper procedures and requirements.

2. Create and Use a Metadata Standard

Simply put, metadata refers to data about data. In particular, to specific information about content and its characteristics. Many organizations struggle to create and keep a metadata standard, even when it can be a foundational component of information governance.

Metadata is essential to remain compliant. For example, it includes vital properties, such as document type, record owners, and dates - something that applies to both electronic and physical records. We mentioned a records retention schedule above. In fact, all the information you need to determine how long to keep a record will be stored in the metadata.

In short, having a metadata standard will help you carry out audit, legal, and regulatory activities and help you determine the data's authenticity and reliability.

3. Document Your Destruction Process

Different industries and sectors will have different policies. We'll go through these methods in the next section, but in terms of best practices, you should always make sure you carefully outline the steps that are necessary to destroy sensitive data records in accordance with them.

The process of documenting these steps can be done collaboratively. It's always a good idea to establish a schedule and best practices stemming from the most elemental level. For example, instructing employees how to deal with the deletion of common files and documents. From there, you can grow to include shredding, secure transportation, and recycling.

If your company is going to use data destruction software, you should make sure everyone has the proper program installed (something an IT specialist will be able to do while also looking at the proper credentials). You should also keep in mind that data will need to be securely erased from a variety of devices, such as PCs, tablets, and smartphones.

4. Validate the Destruction Process

In many cases, destroying data is not enough to ensure it's made truly irretrievable. If you need to comply with a legal mandate or you need to address a potential regulatory issue within your business, you will need to demonstrate the technique you're using for secure data disposal is correctly validated.

One way to determine if your data destruction technique was efficient (in the context of the relevant sustainability and data protection standards), you should always evaluate the results. This will let you not just make sure the data is gone but also calibrate and perfect the method and see whether you need to, for example, carry out maintenance and how often. This is especially the case with physical destruction machines, such as degaussers.

5. Adjust Your Data Destruction Process

This best practice is closely related to the previous one - but goes further. As your business evolves, so will your requirements - including those for dealing with data erasure and device destruction.

An effective data destruction process tends to be lengthy. This means you should never settle for doing things in inflexible ways. Always monitor and adjust your processes to ensure you're keeping up with the latest regulations and policies and preventing your information from falling into the wrong hands.

BEST DATA DESTRUCTION METHODS

Complying with data destruction requirements can feel rather daunting. However, there are many methods you can use to ensure you deal with your physical storage media. Let's go through them in some more detail.

Reformatting

As we previously mentioned, simply deleting a file doesn't erase the data (it only changes how the standard user can access it). Similarly, many people believe formatting a hard drive will completely erase the information. But this, too, doesn't work that way.

Formatting replaces the current file system with another. In a way, you can compare this technique to removing a book's index (but leaving the rest of the pages). Almost anyone can recover the data using software or an online app. So, as far as data destruction methods go, deleting and reformatting is not effective.

File Wiping

File wiping, or data wiping, is all about deleting the information stored in electronic media so users can't access it. This can be accomplished by using software or connecting the drive to a wiping device.

File wiping is quite time-consuming, as obtaining thorough results can take many hours. However, this process (which is more effective than reformatting) also keeps the storage medium available for future use. Still, if you have a large number of hard drives that need to be wiped or you need to comply with more stringent industry regulations, it would be a better idea to use a different method.

File Overwriting

Overwriting uses software to obliterate the data stored in the sectors of a hard drive by overwriting it with (typically) random unreadable information. Usually, a series of 0s and 1s. Security teams can also use their own preferred patterns for the overwrite.

As a data destruction technique, file overwriting can be effective, provided there are several passes made to ensure there's no residual data (or "bit shadow") left. If there's a shadow, the information could be made identifiable again using an electron microscope. This is why, although overwriting is considered a good data destruction technique for smaller businesses, high-security organizations need to make sure the method is done correctly (which also takes considerable time and effort, and can be ineffective if done on broken or corrupt hard drives).

Degaussing

Degaussing is a data destruction method used with magnetic storage media. A strong magnetic field is generated (which has a higher coercivity than the target medium) and rearranges the field direction. This powerful process can neutralize a device, although it will also make it unusable.

Shredding

Shredding is one of the most popular physical destruction techniques to deal with sensitive data erasure. It's also a cost-effective solution that can work on all sorts of devices, including SSDs, tablets, cellphones, thumb drives, and credit card swipes.

For large enterprises, shredding is a great way to erase data quickly and efficiently. For example, if you have a data center that needs to do in-site destruction, you can compare a hard drive shredder as a paper shredding machine. The large machines can break down the storage medium into small electrical and mechanical components, sometimes as small as 2 mm in size. The data contained in these devices is, thus, made irrecoverable.

If you operate in a high-security sector, shredding can ensure total data destruction. Many companies use professional shredding services to make sure not just that the drives are physically destroyed but also to obtain a certificate of destruction.

Crushing, Disintegrating, and Destroying

Disintegrators are used by many organizations to destroy data. These machines use sharp knives (or knife milling technology) to cut the hard drives or devices into small pieces - so thin, in fact, that they can fall through the disintegrator screen.

Compared to shredders, this method is considerably slower. However, the resulting result is much finer.

A similar process, which involves the application of an external force on the media to cause elastic deformations and cracks, is pulverization. Other options include a hard disk destroyer machine (or HDD destroyer machine) and hard drive crushing machine.

Melting

In some cases, a hard drive can be dipped into nitric acid (HNO3) or hydrochloric acid (HCL) to destroy its components. There isn't really any specific equipment built for melting hard drives, but some recycling centers drop the devices on molten steel.

This data destruction method is highly dangerous to both humans and the environment and, therefore, not a recommended option.

DATA DESTRUCTION AND DISPOSAL METHODS

Once you've dealt with the data destruction part of the process, for instance using a hard drive destruction machine, it's time to look at how you can dispose of the resulting components (for example, shredding and disintegrating will result in small fragments you will also need to deal with).

All unwanted media should be sanitized before it moves out of your organization. Not doing so can result in critical data remaining and becoming accessible to others.

There are also environmental considerations when it comes to disposing of destroyed media and devices. Of course, disposing of drives or pieces of them in the trash is not acceptable, as you would contribute to landfill waste. The best idea is to rely on professionals who understand how to properly and securely dispose of the resulting materials.

If you're looking for a specialized data destruction company, check Phiston Technologies. Our innovative solutions (which include HDD destroyers, SSD destroyers, degaussers, and disintegrators) are designed to deal with changing technology and data demands. They will fully destroy a hard drive or any storage device and make the information stored in it 100% unrecoverable and unreadable. Don't hesitate to contact us to discuss a solution fit for your needs.

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.