What is Data Sanitization? Are there any Data Sanitization methods?

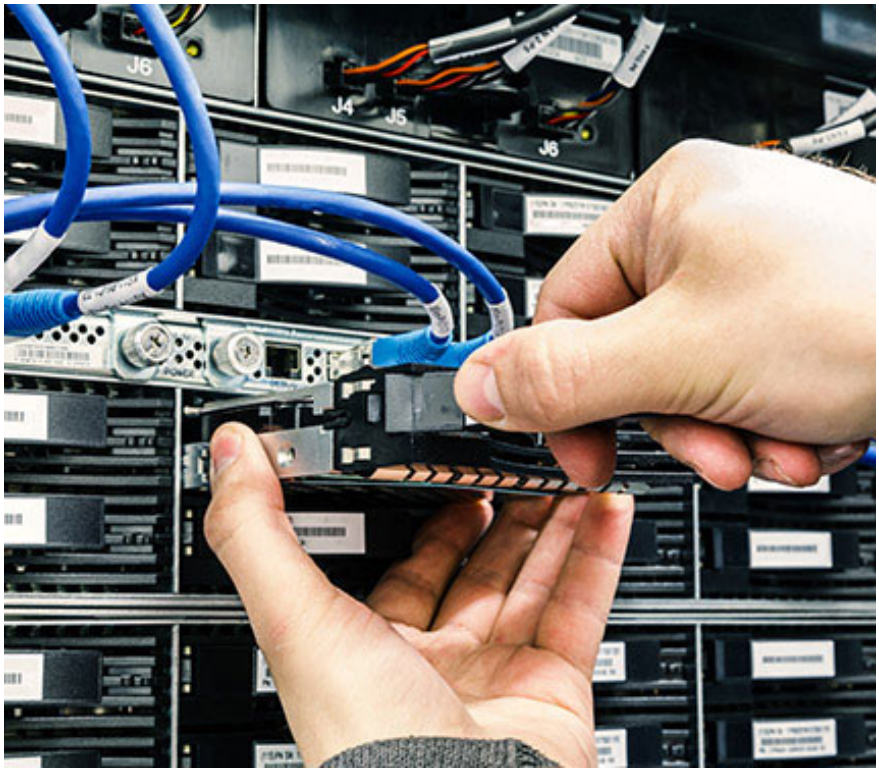
The Data Sanitization method is a specific way in which a data destruction program or file destruction software overwrites data on a hard drive or other storage device.

The Data Sanitization method is a specific way in which a data destruction program or file destruction software overwrites data on a hard drive or other storage device.

Most data destruction programs support a variety of Data Sanitization methods so that users can choose and find out which method is appropriate for the specific data type that needs to be deleted.

Learn about Data Sanitization

What is Data Sanitization?



Data Sanitization is an important step in the data life cycle. Once the data has expired or is considered obsolete, redundant or unimportant, it is important to handle that data securely.

Data Sanitization is the process of intentionally discarding or destroying data permanently stored on the device, in order to make it impossible to recover. A 'sanitized' device does not contain any remaining, usable data. Even with the help of advanced tools, data will never be recovered again.

According to Gartner, there are three methods to perform Data Sanitization: Physical destruction, Cryptographic Erasure (erasing the encryption key of the self-encrypting drive and the encryption algorithm must be at least 128 bits in order for the process to succeed) and Data Erasure (a software-based overriding method that completely destroys all data on the hard drive).

Other names for Data Sanitization

The Data Sanitization method is also commonly known as Data Erasure, Data Wipe, Wipe Algorithms (the process of deleting files, but in reality, does not remove them from the hard drive. Unwanted information may still be on the computer, is available for recovery) and Data Wipe Standard (data deletion standard).

When you see a term like this, that program will talk about Data Sanitization as described here.

Note : Technically, other methods of data destruction not based on software overwriting are also called Data Sanitization methods, but in most cases, this term refers to methods of deletion. Software based data.

Which method does not meet the requirements of Data Sanitization?

The three methods in Part 1 meet the requirements of Data Sanitization, but there are many other data processing methods that do not achieve this. These terms are often used instead, but are not accurate with the conditions of Data Sanitization listed above. These incomplete Data Sanitization methods have not been proven to cause data on storage devices to be unrecoverable.

Incomplete Data Sanitization methods include:

1. **Data Deletion** ('Delete' data)
2. **Data Wiping** ('Wipe' data)
3. **File Shredding** ('Shred' file)

(Further reading: Differentiate Delete and Erase, wipe and shred)

1. **Reformatting** (Format again)
2. **Factory Reset** (**Factory reset**)
3. **Data Purging** (Method of permanently deleting data from storage space)
4. **Data Destruction** (The process of destroying data stored on tapes, hard disks and other types of electronic media so that they are completely unreadable, accessed or used for unauthorized purposes)

None of these methods includes the verification and certification steps required to meet Data Sanitization requirements. When considering a Data Sanitization method for your organization, consider risk tolerance. Strictly regulated industries should choose a complete Data Sanitization method to comply with data privacy and security regulations, as well as minimize the impact of security breaches.

List of Data Sanitization Methods

Here are some common Data Sanitization methods used by data destruction programs and the organization or individual that created the method:

1. **Secure Erase** (the name given to a group of commands available from the firmware on hard drives based on PATA and SATA)

2. **DoD 5220,22-M** (US Department of Defense)
3. **NCSC-TG-025** (United States National Security Agency)
4. **AFSSI-5020** (US Air Force)
5. **AR 380-19** (US Army)
6. **NAVSO P-5239-26** (US Navy)
7. **RCMP TSSIT OPS-II** (Canada)
8. **CSEC ITSG-06** (Canada)
9. **HMG IS5** (UK)
10. **ISM 6.2.92** (Australia)
11. **NZSIT 402** (New Zealand)
12. **VSITR** (Germany)
13. **GOST R 50739-95** (Russia)
14. **Gutmann** (Peter Gutmann)
15. **Schneier** (Bruce Schneier)
16. **Pfitzner** (Roy Pfitzner)
17. **Random Data** (using some data destruction programs to overwrite existing information on hard drives or other storage devices)
18. **Write Zero** (Data Sanitization method relies on Write Zero software to overwrite existing data on storage devices such as hard drives)

Most data destruction programs also allow you to customize your own Data Sanitization method with any template and can override it as many times as you like.

For example, the program may allow you to choose to overwrite data with **zeros** for the first time, **1** for the second and then random characters for another 8 times. This effect is a modified version of the Schneier method, which usually only supports 7 times in a slightly different fashion.

Which Data Sanitization method is best?

Overwriting one or more files or the entire hard drive, each time with a character, will prevent any file recovery methods based on data recovery software from the hard drive. This almost got the consensus everywhere.

According to some researchers, one data override is enough to prevent advanced hardware-based information extraction methods even from the hard drive, meaning that most Data Sanitization methods are overkill. set. But this is not agreed by others.

Most experts agree that Secure Erase is the best way to overwrite an entire hard drive in one go. The very simple Write Zero method does basically the same thing, but is much slower.

Using any method to erase data is really just overwriting other data on the previous data, so that the information is replaced with something useless (each method works this way). . The new data is essentially random and practically does not contain any personal information. That is why the numbers 1, 0 and random characters are used.

If one override is sufficient, why are there so many Data Sanitization methods?

As the article mentioned above, not everyone agrees that the software-based Data Sanitization method will prevent all data recovery methods. Because of advanced hardware-based methods that can extract information from an existing hard drive, some government organizations and researchers have devised certain methods of overwriting data, according to the study. Research, can prevent these advanced recovery methods from working.

What does "acknowledgment of writing" mean?

If you read more about individual Data Sanitization methods, you'll find that most of them have verification after overwriting a character on the data, meaning that they will check the drive to make sure that the content. has actually been overwritten.

In other words, verifying data logging is like checking to see if you actually did this properly.

Some data removal software tools will allow you to change the number of verifications that the file has disappeared. Some options can verify only once at the end of the process (after all overwrites have been completed), while others will verify the writing after each.

To check the entire drive after each overwrite to ensure that the files are being deleted will undoubtedly take longer, because the program must check more often than just once at the end of the process.

Wish you choose the right method!