THE NATIONAL CYBERSECURITY SOCIETY

HOW TO PERMANENTLY DELETE DATA

As a small business owner, it is time to replace your computer hardware and servers. You want to donate the equipment to a local school or homeless shelter. You believe that all the sensitive data from your equipment has been deleted, but how can you be sure? This how-to-guide will explain how to permanently delete data from your laptop, server or removable media.

In modern computer systems, data is not actually deleted from the disk it is stored on. Instead, all pointers to the data are deleted, and the area on the disk is marked as available to be overwritten. This simple, but quick way, to delete data makes it very easy to recover accidently deleted data, but also enables unauthorized personnel access to data that should have been deleted.

STEP 1: IDENTIFY DATA

The first step in any data deletion project is to identify what kind of data needs to be deleted. If the information stored is non-critical, and non-regulated, some of the more advanced techniques may not be necessary, as the process can take a long time. Simply identify the data (on all mediums) and delete.

STEP 2: DELETION – MOST ADOPTED

The most widely adopted method to delete data is to overwrite using a utility that writes a series of 1s or 0s on the whole drive, overwriting any information that was there. Since Operating Systems typically mark the deleted file to be overwritten, simply overwriting the whole disk multiple times is sufficient to deter most attempts at data recovery. Using the overwrite method of data deletion is a Department of Defense approved technique that works on most media, including USB Drives and Flash Media. Industry tools include:

- https://dban.org/
- https://www.bleachbit.org/
- https://www.whitecanyon.com/wipedrive-enterprise

Limitation: Simply overwriting the sectors on a SSD or Flash based array may not

DID YOU KNOW?

- ✓ Data breaches continue to increase each year, outpacing the previous year.
- ✓ One way to minimize the impact of a data breach is to completely remove the data once it is no longer needed - from all sources including your backup.
- ✓ Know what data you have and keep an inventory of it and where it is stored.

Still have questions, need help?
Contact us at our **"Ask-an-Expert"** service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

Data Deletion continued...

be enough to ensure that the data is not recoverable. Some SSDs and Flash media use data managing techniques that may render such methods ineffective.

Please note that while data can be recovered from a disk that has been overwritten, this process typically involves disassembling the disk drive, and inspecting the flash storage module or disk platter itself. [4]

STEP 3 - MOST SECURE

Cryptographic Erase is the most secure method of deleting files from computer disk drives. Cryptographic Erase occurs at the physical disk level, where all of the sectors are encrypted, and then the encryption key is overwritten. This method ensures that none of the data can ever be recovered using any currently known technique. [2]

Some supported SSD drives also have a built in utility (ATA Secure Erase) that supports a complete and unrecoverable deletion of all files [2]. The standard that governs these drives was developed by the National Institute of Standards and Technology (NIST) and is recognized as the unrecoverable way to delete information [3]

Computer or disk manufacturers typically supply Cryptographic Erase and ATA Secure Erase. References for industry tools are provided:

- http://support.lenovo.com/us/en/downloads/ds019026
- http://www.seagate.com/tech-insights/how-to-ise-your-drive-master-ti/
- https://partedmagic.com/secure-erase/

Cryptographic Erase relies on being able to access all parts of the disk drive from a system level and cannot be used on removable media such as USB Drives, or flash cards. ATA Secure erase is not a very friendly tool to use, and may not remove all the data with this method.

STEP 4: CLOUD

As more and more businesses move to the cloud, the traditional techniques that rely on having physical access to the storage media are no longer valid. You should evaluate the terms in your service level agreement for data destruction clauses and make sure they comply with any regulations you may have.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

Data Deletion continued...

The cloud vendors (Amazon Web Services, Microsoft, and Google) are certified by NIST to have recognized data destruction methods and employ a large security team to manage data integrity and security. [1]

STEP 5: ENCRYPTION

Many modern servers and computers employ self-encryption techniques to automatically encrypt and decrypt any data that enters the disk in real time. This makes the Cryptographic Erase of disk drives much quicker, as the data on the drive has already been encrypted to NIST standards, and only the key that is used to access the data has to be overwritten.

Encryption also has the added benefit that it protects data in case the media is lost. If someone loses a laptop or a USB disk that is encrypted, the data on it cannot be accessed without the decryption key. Industry tools include:

- https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-overview
- https://support.apple.com/en-us/HT204837

DISCLAIMER

The tools mentioned here are valid for 2018, and the NCSS will work to ensure this how-to-guide is kept up to date. Some highly regulated industries may require additional steps to be taken, such as obtaining a certificate of data destruction, and companies should seek services that specialize in data destruction so a certification of destruction can be issued.

REFERENCES:

- [1]https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
- [2]http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- [3]https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase
- [4]http://cseweb.ucsd.edu/~swanson/papers/Fast2011SecErase.pdf

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.