COMPRENEW®

RECYCLING ELECTRONICS • PROTECTING DATA • EMPOWERING COMMUNITY

ELECTRONICS RECYCLING AND DATA SECURITY

What is Data Security? Generally in the electronic recycling industry, when we use the term "data security" we are referring to the protection of data contained in devices with memory (such as computer hard drives, smart phones, printers, fax machines) from being accessed by unauthorized persons or entities. Securing the privacy and personal information of people that interact with hospitals, governmental agencies, financial institutions and other businesses is of utmost concern to both the individual and the holder of data. With so much of our personal and financial information being held in computer databases today, data security has become a necessity. Data breaches have become more common in recent years, leading to a growing awareness of what is at risk and prompting more robust strategies for protecting our data by destroying it.

How is Data Destroyed? There are several ways to destroy data. The most sure-fire method is to completely destroy the media within which the data is held. An example of this is to shred the hard drive of a computer. Simply deleting the information is not enough, as someone with the technical know-how can retrieve even deleted data. For healthcare providers and financial institutions, due to the highly sensitive personal information they hold on a high percentage of the population, the law requires a certificate of data destruction by an authorized third-party media sanitization provider.

How Can Data be Destroyed without Completely Destroying the Media? Other non-destructive options for data destruction include sanitizing the media with software or hardware products to overwrite the media's storage space with non-sensitive data. For this method to be truly effective, the process must be repeated to make the data irretrievable. Degaussing is another method that erases the magnetic field of the media, thus erasing the data stored on the device. Which method is used depends upon the needs and preferences of the owner of the device.

Is One Data Destruction Method Better than Another? That depends. In terms of data security, destroying the media that holds the data is the most complete method of sanitizing data. This may be the only option for some businesses due to government regulations. However, in economic terms, overwriting the media's storage space is better as it allows for the reuse of the device, saving the costs related to manufacturing as well as purchasing a new one. For an electronic refurbisher, this method also provides inventory for their refurbishment enterprise and jobs for their employees. For social enterprise electronic recyclers/refurbishers, it provides job skills training opportunities for at-risk populations.

Certified for Data Security, Comprenew offers both media destruction and clearing, or overwriting, of the existing data, depending upon the needs of our customers. At Comprenew, our primary concern when handling used electronic equipment — whether it comes from a business or an individual — is to destroy the data on every device before refurbishing or reselling it. The work of data destruction is performed by our highly trained staff in a secure area and is the first step in the recycling and refurbishment process, before sending a device for further processing within Comprenew. For customers who request it, data destruction is performed at their site.

For more information about data destruction strategies and methods, visit https://www.csoonline.com/article/2130822/it-audit/the-in-depth-guide-to-data-destruction.html.

e-Stewards CERTIFIED · R2 Responsible Recycling · NSF-ISR Registered to ISO 14001 · NSF-ISR Registered to OHSAS 18001 · NIST · Microsoft REGISTERED Refurbisher · HIPAA COMPLIANT