

Do you have piles of hard disk drives (HDDs) and solid-state drives (SSDs) lying around your data center or storage closet? These drives likely contain sensitive data. And if you're not permanently removing that data in a timely manner, you could be putting your business at risk.

Maybe you're planning to physically destroy these drives by sending them to a third-party IT asset disposition vendor, or perhaps you plan to eventually destroy them in-house. In either case, physical destruction is not your only choice for protecting end-of-life data.

Secure data erasure is another option—one that can help you achieve data sanitization and comply with data protection regulations.

Degaussing & Shredding SSDs is Risky Business

Degaussing may be the cheapest and easiest form of physical destruction for drives. However, degaussing removes data by reducing or eliminating unwanted magnetic fields. But, because SSDs don't store data magnetically, degaussing does not achieve data sanitization.

Physically shredding SSDs can also be an issue because of shred size. The U.S. National Security Agency recommends a shred width of 2mm or smaller to break through the small memory chips and securely remove the data. Most standard industrial shredders produce much larger fragments—leaving information behind.

Physical destruction can also be harmful to the environment by leaving shredded assets behind. Why not reuse your assets and save the planet in the process? You'll also save money you otherwise would have spent on purchasing new storage devices.

Eliminate Risk with Data Erasure

Data erasure is the software-based method of securely overwriting data from any data storage device using zeros and ones onto all sectors of the device. By overwriting the data on the storage device, the data is rendered unrecoverable. At the end of the erasure process, the data erasure software will verify that data has been successfully overwritten across all sectors of the device. Then, the software will produce a tamper-proof, auditable certificate that the erasure has been successful. At this point, data sanitization has occurred. Data erasure can be done on-site or remotely and offers better control than other forms of data sanitization. The process can also be automated to save time.

Data erasure is the best way to achieve data sanitization, due to the validation process to ensure the data was successfully overwritten and the auditable reporting readily available. Data erasure also supports environmental initiatives, while allowing organizations to retain the resale value of their storage devices.

[Blancco Drive Eraser](#) allows organizations to securely erase sensitive data in order to safely resell, re-purpose or dispose of both SSDs and HDDs.

Simplify Processes with Patented SSD Erasure

Our patented SSD erasure method is specifically designed to handle functionality differences across a myriad of SSD vendors. It includes:

- A multi-phase, proprietary SSD erasure approach that uses all available SSD-supported security protocols
- Automated techniques to remove system BIOS freeze locks, enabling access to key internal SSD security features
- Procedures that root out drives that give false positives about their internal erasure processes
- Third-party benchmark testing and validation
- A comprehensive, tamper-proof report to confirm erasure results and prove compliance

Reasons to Choose Blancco Drive Eraser for HDDs and SSDs

- Allow your IT administrator(s) to erase data, reducing risk by keeping your sensitive data out of the hands of a third-party
- Achieve error-free, certified erasure reporting with a 100% verifiable audit trail
- Save money by securely erasing and reusing drives instead of physically destroying them
- Save on physical destruction costs with more affordable data erasure software
- Securely erase multiple drives simultaneously, saving time for other business-critical initiatives
- Stay compliant with state, federal and international data privacy regulations and guidelines, including ISO 27001 and ISO 27040

Learn more about [Blancco Drive Eraser](#). Get your [free trial](#) now.