Secudrive Drive Eraser

The easiest and most cost-effective secure drive erase software for your PCs, laptops, servers, and external hard drives, USB flash drives, and SSDs.

Why Secudrive Drive Eraser?

Secudrive Drive Eraser is a drive-wiping solution for enterprises with over 20 internationally certified data-wiping algorithms, designed to completely erase various storage devices beyond scope of recovery. It enables organizations to comply with Sarbanes-Oxley, GDPR, PCI-DSS, GLB, HIPAA, and more.

Secudrive Drive Eraser generates logs and reports on drive-erasure tasks including computer, drive, and erasure information for post-audit. The logs and reports can be transferred to an enterprise IT asset management system so that the drive wiping can be managed with it integratedly.

Secudrive Drive Eraser makes disk wiping easier. It is a USB drive-type solution. Even a nonspecialist can process wiping procedures without any additional BIOS/UEFI set up after plugging the USB drive into a PC. It can wipe multiple external drives connected to a PC as well as multiple disks in a PC in parallel with high speed. It can wipe multiple PCs simultaneously. It can completely erase all drives of Windows, Mac, and Linux machines.

Why Data Destruction Using Data Erasure Software?

- For data destruction, more and more organizations use data erasure software instead of physical destruction such as degaussing and physical shredding to not only cut cost but also enhance security.
- Data erasure using software is more economical and more eco-friendly than physical destruction because it makes the storage reusable while the wiped data are unrecoverable. Whereas physical destruction involves risks of loss or theft during disassembly, storage, or moving to a separate warehouse, hassle-free data wiping using software at the location of the storage itself eliminates with such risks. Furthermore, software can automatically generate tamper-proof reports about the data erasure task, while physical destruction produces no manageable evidence. Data erasure using software is recognized as even more secure than physical destruction.

	Secudrive Drive Eraser	Physical Destruction
Data	**Unrecoverable**	Unrecoverable
Device	**Reusable, resellable**	Trash
Report for audit	**Tamper-proof**	Vulnerable evidence
IT asset management	**Easy data integration**	Manual management
Workplace*	**On users' desks**	Warehouses
When to erase	**Move after erasure**	Move and destroy
Data breach risk	**Minimal**	Relatively high during moving/storage

*Secudrive Drive Eraser can wipe drives separately stored in a warehouse, too. However, Secudrive recommends wiping before moving machines to a warehouse to improve security.

+ Major Features and Benefits

Effortless data erasure

- When a machine is logged onto Windows, a user can wipe all data including the OS by running the .exe program without any additional CD/USB booting
- Even a nonspecialist can manage easily
- Supports USB booting to wipe Windows, Mac, and Linux machines

Log and report

- Creates a detailed log and report about the computer, storage, and erasure task
- Generates a tamper-proof report for post-audit
- Logs can be integrated with the asset management system

Reliable and fast data erasure for all

- Wipes various types of OSs and storages
- Supports more than 20 international standard data wipe algorithms
- Wipes multiple PCs simultaneously
- Wipes multiple drives in parallel at high speed by using multithread technology
- Detects and wipes DCO/HPA hidden areas
- Wipes detected RAID
- Wipes SSD (Solid State Drive). Supports "Secure Erasure" for life extension of SSD

Various convenient add-ons

- Shows %-type S.M.A.R.T. index of a drive to check if the drive is reusable
- Provides estimated remaining time for each erasure algorithm
- Provides hexadecimal view to verify erasure taskorithm
- Supports CLI (Command Line Interface) mode
- Manages erasure task history per each operator
- Additional licenses can be purchased via email

+ Technical Specification

Effortless data erasure

- Erases all x86 and x64 architecture computers (Windows, Mac, and Linux)
- Erases drives such as ATA/IDE, SSD, SATA, SCSI, FireWire
- Erases SSDs such as SATA, M.2, and NVMe

Support international standard erasure algorithms

- One pass zeros
- One pass random
- US DoD 5220.22-M
- US DoD 5220.22-M(ECE)
- US DoE M205.1-2
- Canadian OPS-II
- Canadian CSEC ITSG-06
- German VSITR
- Russian GOST p50739-95
- US Army AR380-19
- US Air Force 5020
- British HMG IS5 Baseline
- British HMG IS5 Enhanced
- Navso P-5329-26 RL
- Navso P-5329-26 MFM
- NCSC-TG-025
- NSA 130-2
- Bruce Schneier
- Gutmann
- NIST 800-88
- Australian ISM-6.2.93

and more

+ Use Cases

- **Integrated data-wiping management before disposal or reuse of various storage for enterprises**
  Generates reports after wiping and integrates the information into an asset management system

- **Data wiping of out-sourced computers after a project**
  Prevents data breach after a project
  Wipes data by outsourcer and audits with a tamper-proof report

- **Integrated management of data wiping of PCs in scattered branch offices where there is no IT professional**
  Safely move storage to headquarters or warehouse after wiping
  Transfer wiping report to headquarters after wiping and integrate it with asset management