Pre-Sale Device Checklist: Complete Data Sanitization Guide

Protect Your Personal Information Before Selling or Donating







Why This Matters

- ▲ Factory resets & file deletion don't actually remove data they just hide it
- Professional recovery tools can restore "deleted" files, credentials, financial records within minutes
- Proper sanitization ensures your personal information is permanently destroyed

! Data Exposure Risk

Selling without proper sanitization exposes: login credentials, financial records, personal photos, sensitive documents







Pre-Sanitization Preparation

- Identify Your Storage Devices
 SSD (Solid State Drive): Standard in devices from 2015 onward
 HDD (Hard Disk Drive): Spinning magnetic disk, common in older devices
 External drives: USB-connected hard drives, flash drives, SD cards
 Check storage type: Windows (Device Manager) or Mac (About This Mac)
- Remove Hardware Locks & Accounts

 Remove BIOS/UEFI passwords if set

 Remove firmware locks (especially Mac Activation Lock)

 Deregister device from manufacturer accounts

 Remove device from "Find My" services

 Clean device exterior and remove personal identifiers

SSDs and HDDs require completely different sanitization methods

Pre-Sanitization Preparation

	Disconnect & Disable Services
Back up files to separate external drive or cloud service	Disconnect from internet (disable WiFi, unplu Ethernet)
 Verify backup integrity by opening several files Store backup drive in secure location separate from device 	 Disable cloud sync services (OneDrive, iCloud Google Drive) Temporarily disable antivirus and security software Log out of all accounts (Microsoft, Apple ID, Google, social media)
	Remove disk encryption recovery keys from

A Sanitization permanently destroys all data.

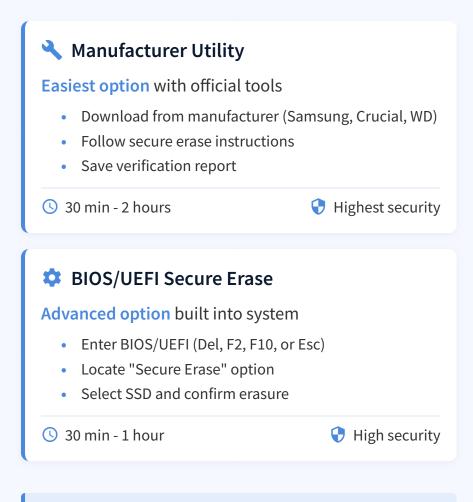
There is no recovery after this process.

Cloud services may attempt to sync or recover data during sanitization, interfering with the process

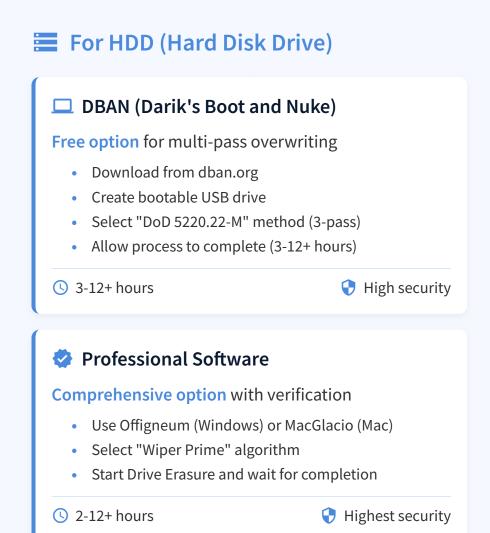
cloud storage

Choose Your Sanitization Method

For SSD (Solid State Drive)



Traditional file deletion and multi-pass overwriting do not work properly on SSDs due to wear-leveling algorithms



Phase 3: Post-Sanitization Verification Internal SSD or HDD: Sanitized (Yes/No) External hard drive(s): Sanitized (Yes/No) USB flash drive(s): Sanitized (Yes/No) SD cards: Sanitized (Yes/No)



Common Mistakes to Avoid



Factory resets only delete file pointers, not actual data



Use hardware secure erase or multi-pass overwriting

DBAN on SSDs

DBAN doesn't work properly on SSDs due to wear-leveling SSD-Specific Tools

Use manufacturer utilities or professional software

Forgetting External Drives

External drives often contain years of backup data

Complete Inventory

Sanitize every storage device connected to your computer

Encryption ≠ Sanitization

Encryption protects data but doesn't erase it

Always Sanitize

Perform secure erasure even on encrypted drives





Offigneum

Windows

- Supports all device types: SSDs, HDDs, external drives, USB
- 51 sanitization algorithms including Wiper Prime
- Enterprise-grade verification reports

www.ambeteco.com/Offigneum



MacGlacio

Mac

- Professional-grade sanitization for all Maccompatible storage
- Optimized for SSDs and HDDs with proper methods
- Supports USB sticks, SD cards, and external drives

www.ambeteco.com/MacGlacio



For Free Options



Manufacturer SSD Utilities

Samsung, Crucial, WD, Kingston

- Samsung Magician, Crucial Storage Executive, WD Dashboard
- Manufacturer-specific secure erase commands
- Free and optimized for specific SSD models



DBAN

HDD Only

- DoD 5220.22-M multi-pass overwriting method
- Bootable utility that works outside of OS
- A Not suitable for SSDs only works on HDDs

Your personal data is your responsibility

- One forgotten device can expose financial records and personal photos
 - Proper sanitization prevents identity theft and privacy breaches
 - Follow this checklist to ensure complete data destruction

Data Sanitization is Not Optional—It's Essential





