

DATA DESTRUCTION

How to choose the right method, understand the standards, and prove the work was done.

Every retired storage device eventually reaches the same question:
what must happen to the data before the device can leave your control?



The answer depends on the storage technology, the sensitivity of the information, applicable requirements, and your organization's security policies.

The goal is simple: **match the destruction method to the media, the data, and the risk.**

NIST SP 800-88 Rev. 2: THE FRAMEWORK BEHIND THE DECISION

NIST SP 800-88 Rev. 2 provides federal guidance for media sanitization. It defines three levels of action based on information sensitivity and risk.

✓ CLEAR

Logical technique that sanitizes data while generally allowing the media to remain usable.

✓ PURGE

More robust sanitization that makes recovery infeasible using state-of-the-art techniques. Common methods include cryptographic erase and, for magnetic media, degaussing.

✓ DESTROY

Physical techniques that make recovery infeasible and leave the media incapable of being used again for data storage.

KNOW THE DIFFERENCE

	NIST SP 800-88	Sanitization guidance and media destruction methods.
	NAID AAA	Third-party certification for secure information destruction.
	NSA EPL	Evaluated equipment requirements.
	R2v3	Responsible e-waste management and downstream accountability.

AUDIT-READY DOCUMENTATION



Physical destruction addresses the media. Documentation addresses the audit.

A defensible record should include:

- ✓ Device and serial number
- ✓ Destruction method, date, and location
- ✓ Chain of custody and reconciliation
- ✓ Certificate of Destruction

CAPTURING THE EVIDENCE BEFORE DESTRUCTION

DriveSnap AI™ photographs HDD and SSD labels and extracts serial numbers to create a device-level digital record before destruction.

LABEL PHOTO

AI PHOTO CAPTURE

SERIALIZED RECORD

DESTRUCTION

CERTIFICATE OF DESTRUCTION

MATCH THE METHOD TO THE MEDIA

According to NIST SP 800-88, different storage technologies require different destruction methods. Magnetic media and flash media store data differently, so they cannot be processed the same way.

MAGNETIC MEDIA

HDD • TAPE • FLOPPY



DEGAUSSING

Exposes magnetic media to a powerful magnetic field that erases stored information. On HDDs, it also erases the factory-written servo information required for operation, leaving the drive permanently unusable.

Choose when: Magnetic media requires controlled sanitization and reuse is not intended.



HDD SHREDDING

Mechanically shreds hard disk drives into strips, destroying the platters, electronics, and mechanical components. The resulting material cannot be reconstructed into a functional storage device.

Choose when: Policy requires destruction, drives are failed or obsolete, or large HDD volumes require efficient processing.



DEGAUSS + SHRED

Combines magnetic sanitization with physical destruction for high-security HDDs. NSA/CSS guidance requires approved degaussed HDDs to also undergo physical destruction that deforms the platters.

Choose when: Policy, classification, or contract terms require layered high-security destruction.

SOLID-STATE & FLASH MEDIA

SSD • USB • MOBILE



Batteries must be removed from mobile devices before destruction to reduce fire risk.



COMMERCIAL DISINTEGRATION

Reduces SSDs, USB drives, memory cards, smartphones, tablets, and other flash media into small particles.

Choose when: Physical destruction is required but NSA EPL equipment is not specified.



NSA EPL 2mm DISINTEGRATION

Uses evaluated equipment to reduce applicable solid-state media to the required particle size of 2 mm or less.

Choose when: Policy, classification, or contract terms specify NSA-evaluated destruction equipment.

What is the NSA EPL?

The NSA Evaluated Products List identifies specific equipment evaluated against NSA/CSS requirements for designated media types. EPL listing applies to the equipment, not the vendor.



CERTIFICATE OF DESTRUCTION

The final record confirming that media was processed through the designated destruction method.

You should be able to prove what was destroyed, how it was destroyed, and when it happened.

Speak with a Data Destruction Specialist



(800) 731-1909



securis.com