Resource · Checklist

NIST 800-88 Data Destruction Checklist

Updated for 2026 · Aligned to NIST SP 800-88 Rev. 1

What 800-88 actually is

NIST Special Publication 800-88 Rev. 1, *Guidelines for Media Sanitization*, is the U.S. federal standard for making data on storage media unrecoverable. It is the de facto baseline cited in HIPAA guidance, PCI-DSS, GLBA examinations, and most enterprise procurement contracts. It defines three sanitization categories — **Clear**, **Purge**, and **Destroy** — based on the confidentiality of the data and the type of media.

The decision matrix

Category	Use when…	Methods
Clear	Low confidentiality. Media stays inside the organization.	Overwrite, factory reset, built-in secure erase. Unreliable on SSDs.
Purge	Moderate confidentiality. Device may change ownership.	Cryptographic erase, ATA/NVMe Sanitize, degaussing.
Destroy	High confidentiality, or Purge not feasible.	Shred to defined particle size, disintegrate, incinerate, melt.

The 7-step checklist

Step 1. Inventory every device.

Device type · manufacturer · model · serial number · capacity · encryption status · current physical location. Anything not on the list never gets sanitized.

Step 2. Classify the data.

Map each device to a confidentiality level (Low, Moderate, High). Default to Moderate when unsure; step up for regulated workloads.

Step 3. Select the method.

Apply the Clear / Purge / Destroy matrix. Confirm the method is supported by the device — many SSDs falsely report secure-erase success.

Step 4. Execute the sanitization.

Use vendor-supported tools. Capture tool logs and operator identity. Maintain chain of custody from removal to sanitization to disposal.

Step 5. Verify a sample.

Minimum 10% of devices; 100% of devices holding High-confidentiality data. For physical destruction, verify shred particle size with calipers.

Step 6. Issue Certificates of Destruction.

One per device or per batch. Include serial numbers, method, NIST category, operator, witness, date, location, and reference to verification record.

Step 7. Update the asset register and retain records.

Mark assets sanitized and disposed. Retain certificates for the longest of: your retention policy, regulator requirements, or seven years.

Five mistakes we still see in 2026

- **Treating SSDs like HDDs.** A DBAN-style overwrite does not reliably sanitize an SSD.
- **Trusting the device's "secure erase" report.** Many consumer SSDs return success without sanitizing over-provisioning.
- **No serial-number-level certificate.** A certificate that says "destroyed 47 drives" without serials is unusable in an audit.
- **Skipping the inventory step.** If you don't have a list, you can't prove anything was sanitized.
- **Mixing destruction and resale streams.** Once a device is on the destroy path, it cannot reappear on the resale market.

Need help executing?

CCRAMM Technical Services performs NIST 800-88 aligned destruction on-site or at our facility, with serial-number-level Certificates of Destruction for every device. Visit ccrammts.com/pages/data-destruction.html or call (717) 884-8835.