Data Sanitization Policy

[Organization name]. Built on NIST SP 800-88 Rev. 2, Guidelines for Media Sanitization (September 2025). To adopt it: fill in every highlighted blank, delete the grey guidance lines, then have it approved and dated in Section 14.

Document control	
Organization	[Legal name]
Sites covered	[Addresses of every site that handles media]
Policy owner	[Name, job title]
Approved by	[Name, job title]
Version / effective date	[1.0] / [date]
Next review due	[date]

1. Purpose NIST 4

This policy sets how [Organization] sanitizes data storage media before the media is reused, sold, donated, returned, recycled or destroyed. Its goal is that no data can be recovered from media once it leaves our control. It sets the minimum method for each kind of data, who does what, how results are checked, and which records we keep.

A step-by-step bench procedure for each tool and media type sits under this policy: [procedure document name or location].

2. Scope NIST 4.2, 4.3.1

- Covers all storage media that holds, or may hold, [our data / our customers' data]: hard drives, SSDs (SATA and NVMe), USB drives and memory cards, phones and tablets, [servers, printers, network equipment with storage] and [paper records].
- Covers media we own and media we receive from customers for processing at [site(s)].
- Each device is checked for every storage component it contains. One computer can hold more than one drive.
- We sanitize the whole storage device. Sanitizing only part of a device needs written approval from [job title].
- Out of scope: [exclusions, e.g. sealed, unopened retail software media].

Guidance: NIST prefers sanitizing the whole device, because data on part of a drive can spill into remapped or spare areas (Sec. 4.2).

3. Roles and responsibilities NIST 4.7, 4.1

Role	Responsible for	Who (name or job title)
Policy owner	Keeps this policy current; approves exceptions	[ ]
Technician	Sanitizes media and records the result	[ ]
Validator	Approves or rejects each result. Must not be the technician who did the work.	[ ]
Asset manager	Tracks every device from intake to its final destination	[ ]
Records owner	Keeps the records; checks that sanitization never destroys records we must keep	[ ]
Privacy lead	Advises on media that holds personal data	[ ]

Guidance: one person may hold several roles, except that the validator must be someone other than the technician for that piece of media.

4. Classify the data first NIST 4.3, 4.3.2, 4.1

Before sanitization, each device or batch gets a confidentiality category: Low, Moderate or High, using [our classification scheme / the category the customer states in the contract].

Category	What it covers here
Low	[e.g. public information, no personal data]
Moderate	[e.g. internal business data, limited personal data]
High	[e.g. health, financial or payment data, credentials, regulated personal data]

If the category is not known, the media is treated as [High].

5. Minimum method by category and destination NIST 4.3, Fig. 1, 4.3.3, 4.3.4

	Stays under our control	Leaves our control
Not going to be reused	Destroy	Destroy
Low	Clear	Purge
Moderate	Clear	Purge
High	Purge	Destroy

- Media leaves our control when it is sold, donated, returned at the end of a lease, exchanged under warranty or sent to a recycler.
- Media held by a contracted maintenance provider whose contract protects the data's confidentiality stays under our control.
- We may always apply a stronger method than the table. A weaker one needs written risk acceptance from [job title] (Section 12).
- Media that is damaged, and can't complete a logical Clear or Purge, is destroyed.

Guidance: the table is NIST's decision flow (Fig. 1). Clear protects against recovery through the drive's normal interface. Purge makes recovery infeasible even with laboratory techniques and can leave the drive reusable. Destroy also makes recovery infeasible, and the drive can't be used again (Sec. 3.1).

6. Approved techniques by media type NIST 4.4, 3.1, 4.1

The category sets the method. The media type sets the technique. Techniques must comply with IEEE 2883 or [another standard we accept].

Media type	Clear	Purge	Destroy
Hard disk drive	Overwrite all user-addressable space	Device sanitize command; degauss only with a degausser rated for the drive	[Shred / disintegrate / crush]
SATA or NVMe SSD	Overwrite (does not reach spare cells)	Device sanitize command: block erase or cryptographic erase. Never degauss.	[Shred / disintegrate]
USB drive, memory card	Overwrite	[Usually none available]	[Shred]
Phone, tablet, office equipment	Factory reset, if the device then gives no way to read the old data	[Per manufacturer]	[Shred]
Paper	Not allowed	Not allowed	[Cross-cut shred / pulp / incinerate]

- Cryptographic erase is used only where [job title] has confirmed the drive meets NIST Sec. 3.2.
- When Purge is required and the media has no Purge technique, the media is [destroyed].

7. Tools and equipment NIST 4.1, 4.6

Only tools on this list are used. A new tool, or a new version of a listed tool, is tested by [job title] before use: [how it is tested].

Tool or equipment	Version	Used for	Last tested / calibrated	Approved by
[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]

- Shredders and degaussers are calibrated and maintained [schedule].
- We ask tool vendors for [assurances, e.g. test results or independent certification].

8. Verification: did it complete? NIST 4.5.1

- After every Clear or Purge, the technician checks the tool's completion status, any errors or anomalies, and the health of the media.
- After Clear or Purge, we also read back [__ %] of each drive's user-addressable space and confirm it holds the expected result.
- After Destroy, the technician inspects the remains against our maximum particle size of [ ] and records the equipment used.
- Quality check: every [week / month], a competent person who did not sanitize the media tests [__ %] of sanitized media with data recovery software. The sample covers every media type, tool, technician and station.

Guidance: NIST says elaborate sampling after Clear or Purge is not necessary unless your policy requires it (Sec. 4.5.1), so the read-back percentage is your decision; write 0 if you rely on completion status alone. R2v3 facilities: SERI's guidance quotes Appendix B (13), which requires at least 5% of logically sanitized media to be sampled by a competent, independent party.

9. Validation: is the result acceptable? NIST 4.5.2

The validator reviews each result and approves or rejects it. A result is rejected when:

- the tool reported errors, or parts of the media could not be reached;
- the technique was wrong for the media or the category (for example, degaussing an SSD);
- the person was not trained, or the tool was not approved or not calibrated;
- the outcome is below this policy's minimum (for example, shred particles too large);
- the scope was too narrow (for example, a plain overwrite on an SSD with spare capacity).

Rejected media is sanitized again with a different technique, or escalated to a stronger method, and checked again. If a quality check finds recoverable data, [job title] stops the affected process, re-checks media processed since the last clean check, and opens a corrective action under [procedure].

10. Records NIST 4.6, 4.3.6, 4.7.8

A certificate of sanitization, paper or electronic, is completed for each storage device. It records at least: manufacturer, model, serial number, our asset number, media type, media source, category (optional), method, technique, tool and version, verification method, and the name, title, date, location, contact details and signature of the people who verified and validated.

- We also record the media's destination: [reuse / resale / recycler / manufacturer], and to whom.
- Each device is tracked at intake, when it leaves its last place of use, and at its final destination.
- Records are kept in [system or location] for [retention period], as set by [the records owner, customer contracts and the laws that apply to us].
- After successful validation, old confidentiality markings are removed from media whose category is now lower.

Guidance: NIST sets no retention period. Ask your records owner, check your customer contracts and the laws that apply to you, and write the longest period that applies.

11. Training NIST 4.1, 4.5.2

Nobody sanitizes or validates media until trained on [this policy, the procedure, each tool they use] and signed off by [job title]. Refresher training every [period]. Training records are kept with the sanitization records.

12. Exceptions NIST 4.3

Any departure from this policy needs written approval from [job title] before the work is done. The approval records the media, the reason, the risk accepted and when the exception ends.

13. Review NIST 3.1

This policy is reviewed every [12 months], and sooner when we adopt a new media type, tool or tool version, when a quality check fails, or when a law or customer contract changes.

14. Approval

Approved by	
Name	
Job title	
Signature	
Date	

Revision history

Version	Date	What changed	Approved by
[1.0]	[ ]	First issue	[ ]

Where each section comes from

Every section of this policy maps to a section of NIST SP 800-88 Rev. 2.

Policy section	NIST SP 800-88 Rev. 2	What NIST covers there
1. Purpose	4	A sanitization program and what it should include
2. Scope	4.2, 4.3.1	Whole-device vs partial sanitization; every storage component in a device
3. Roles	4.7	Roles and responsibilities
4. Classify the data	4.3, 4.3.2	Decisions follow the confidentiality of the data, not the media type
5. Minimum method	4.3, Fig. 1, 4.3.3-4.3.4	Reuse, control of media, decision flow
6. Techniques	3.1, 4.4	Clear, Purge, Destroy; comply with IEEE 2883
7. Tools	4.1, 4.6	Tool use, calibration, testing; tool and version on the record
8. Verification	4.5.1	Did the technique complete; sampling only if policy requires
9. Validation	4.5.2	Approve or reject; reasons to reject
10. Records	4.6, 4.3.6, 4.7.8	Certificate fields; record the decision; retention advice
11. Training	4.1, 4.5.2	Competencies, skills and training
12-13. Exceptions, review	4.3, 3.1	Risk decisions; techniques updated as storage changes

Structure: NIST SP 800-88 Rev. 2, Guidelines for Media Sanitization (September 2025), Section 4 and Figure 1. R2v3 sampling: SERI, "Verifying the Effectiveness of the Data Sanitization Process".

Free template from reCore (recore.replugit.com). Not legal advice; adapt it to your contracts and the laws that apply to you.