

Media Sanitization Policy Template

A free, adaptable template covering sanitization methods by media type, verification and validation, a certificate of sanitization, vendor requirements, and SOC 2 / ISO 27001 / HIPAA / PCI DSS / GDPR alignment.

Company: _____

Effective date: _____

Policy owner:

Review cycle: Annually, and whenever storage systems or vendors change

HOW TO USE THIS TEMPLATE

Replace every bracketed placeholder with your organization's specifics and adapt the media table to your real inventory. Route the finished policy through your normal approval process. This template is a starting point, not legal advice. See ComplyJet's [Media Sanitization Policy guide](#) for the reasoning behind each section.

1. Purpose

This policy defines how [Company Name] makes data unrecoverable on storage media, and on paper, before that media is reused, returned, donated, recycled, or disposed of. It aims to prevent unauthorized disclosure of information from media that leaves, or has left, the company's control, and to produce a record that proves each sanitization happened.

2. Scope

This policy applies to all storage media owned, leased, or managed by [Company Name], and to hard copy, regardless of location. In scope: laptops and desktops, servers, phones and tablets, USB and removable media, backup media, printer and copier storage, optical discs, paper, and virtual or cloud storage volumes. It applies to employees, contractors, and vendors handling this media. Retention periods are set in the [Data Retention Policy]. This policy governs how data is destroyed once retention has ended or media is retired.

3. Roles and Responsibilities

Role	Responsibility	Name
Policy owner	Maintains this policy, approves exceptions, reviews vendor certificates	[Name]
Sanitization operator	Applies the method, completes the certificate	[Name]

Verifier	A person other than the requester who verifies and validates the result	[Name]
Asset owner	Requests retirement and confirms the media is in the asset inventory	[Name]
Leadership	Approves the policy and any risk acceptance	[Name]

4. Sanitization Methods

Methods follow NIST SP 800-88 Rev. 2, Guidelines for Media Sanitization (September 2025). Revision 1 was withdrawn on September 26, 2025.

Method	Definition	Use when
Clear	Logical techniques (overwrite or reset) that protect against simple, non-invasive recovery through the normal interface	Media is reassigned internally to a user cleared for the same classification
Purge	Physical or logical techniques that make recovery infeasible using state-of-the-art laboratory techniques, leaving media potentially reusable	Media leaves company control and holds Confidential or Regulated/Restricted data
Destroy	Physical destruction (disintegrate, incinerate, melt, pulverize, shred) that makes recovery infeasible and ends the media's use for storage	Media has failed or is obsolete, cannot be validated, or holds the most sensitive data; all hard copy

5. Method by Media Type

Media type	Default method	Fallback	Your decision
HDD (laptop, server)	Purge (vendor sanitize command) or cryptographic erase if fully encrypted	Destroy	[]
SSD and NVMe	Cryptographic erase or dedicated sanitize command. Do not degauss.	Destroy	[]
Phone and tablet	Cryptographic erase plus factory reset; remove from MDM	Destroy	[]
USB and removable media	Purge if supported	Destroy	[]
Backup tape	Purge, or destroy	Destroy	[]
Printer and copier storage	Vendor reset, then purge or destroy on retirement	Destroy	[]
Paper and optical discs	Destroy (cross-cut shred, pulp, incinerate)	None	[]

Cloud and virtual volumes	Cryptographic erase and account deprovisioning	Contractual deletion evidence from provider	[]
---------------------------	--	---	-----

WATCH OUT

Degaussing applies only to magnetic media, must be matched to the media, and does not sanitize SSDs. Overwrite-only methods are not sufficient for flash media with spare or overprovisioned cells. Deleting files or formatting is not sanitization.

6. Cryptographic Erase

Cryptographic erase may be used only where the media was encrypted with strong, company-approved cryptography from first use, the keys were never stored on the same media, and the keys are sanitized or made inaccessible as part of the procedure. The operation must be recorded. Key and encryption requirements are set in the [Data Encryption Policy].

7. Verification and Validation

Verification confirms that the technique completed: tool completion status and errors are checked, or the remnants of a destroyed device are inspected. **Validation** confirms the data was effectively sanitized, and ends in a decision to approve or reject. A rejected result is repeated with a different technique or escalated to a stronger method. Verification and validation are performed by [Verifier role], not the requester.

8. Certificate of Sanitization

A certificate (paper or electronic record) is completed for every device or item sanitized, with at least the fields below.

Field	Entry
Manufacturer, model, serial number	
Asset tag / property number	
Media type and source (user, computer)	
Data classification before sanitization (optional)	
Method (clear, purge, destroy) and technique (overwrite, block erase, cryptographic erase, shred, etc.)	
Tool used, including version	
Verification method	
Verified and validated by: name, title, date, location, contact, signature	

Certificates are retained for [retention period] in [record location].

9. Media Leaving Company Control

Return of leased hardware, warranty or RMA exchange, donation, resale, and recycling all count as leaving company control. Media holding Confidential or Regulated/Restricted data must be sanitized by purge or destroy before it leaves, unless a written contract with the recipient specifically provides for the confidentiality of the information and the policy owner has approved it.

10. Third-Party Vendors

- Complete due diligence on any disposal or ITAD vendor before use, and record the outcome.
- The contract must require sanitization to NIST SP 800-88 Rev. 2 (or an equivalent stated standard) and documented evidence of deletion.
- The vendor must supply a certificate listing serial numbers, method, date, and a named person for every item.
- The company maintains its own record of every disposed item and reconciles it against vendor certificates.

11. Records and Asset Tracking

Media is recorded in the asset inventory when it enters the environment, when it leaves its last location, and when it reaches its post-sanitization destination. Sanitization records are kept so that the company can show all retired media was sanitized, not only some.

12. Exceptions

Exceptions require written approval from [Policy Owner], a documented compensating control, and a review date. All exceptions are logged.

13. Framework Alignment

Framework	Reference	Addressed in
SOC 2	CC6.5 (discontinuation of protections only after data is unrecoverable); C1.2 (disposal of confidential information)	Sections 4 to 8, 11
ISO 27001:2022	Annex A 7.10 (storage media), 7.14 (secure disposal or re-use of equipment), 8.10 (information deletion)	Sections 4 to 11
HIPAA	45 CFR 164.310(d)(2)(i) disposal and (ii) media re-use (Required); (iii) accountability and (iv) data backup (Addressable)	Sections 4 to 9, 11
PCI DSS 4.0	Requirements 9.4.6 (hard copy) and 9.4.7 (electronic media)	Sections 4, 5
GDPR	Article 5(1)(e) storage limitation; Article 17 erasure	Sections 2, 4 to 8

14. Review and Enforcement

The policy owner reviews this policy at least annually and whenever storage systems, data classifications, vendors, or the referenced standards change. Violations may result in disciplinary action up to and including termination of employment or contract.

ComplyJet Media Sanitization Policy Template. Free to adapt for your organization. This template is a starting point, not legal advice.
Reference: NIST SP 800-88 Rev. 2, <https://csrc.nist.gov/pubs/sp/800/88/r2/final>