Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/media-sanitization-checklist/

STANDARDS PREPARATION CHECKLIST

Media Sanitization and Equipment Retirement

Prepare a risk based sanitization program and the records needed to explain decisions about reuse, transfer and disposal.

Baseline: NIST SP 800-88 Rev. 2, with July 2026 FAQ. Prepared November 1, 2026.

Use the questions to prepare the review

This is a planning checklist that prepares the decisions behind an erasure procedure. Preserve material subject to a hold or other retention decision first, then authorize destructive work. Media specific techniques are carried out by qualified personnel under approved procedures.

For this media retirement decision, note which answers rest on a record you can locate and which your team is still confirming. Name an owner for each open question and note why anything is excluded.

Keep encryption keys and confidential device contents in the authorized owner's controlled records. Keep preservation and disposal records with the authorized owner.

Use these selected media retirement decision questions to prepare a discussion. The references support the topics.

© 2026 Global Digital Forensics, Inc. All rights reserved.

MS-01

Has the owner authorized disposition and checked retention needs?

Confirm what may be erased or destroyed and whether the business or its legal team requires material to be retained. Sanitization is designed to be permanent, so retention is settled first. This preservation decision is a GDF preparation step that sits alongside the NIST guidance, with legal hold duties set by counsel.

Evidence to gather

Authorized disposition scope, information owner and any preservation/retention instructions.

To complete the record

Reconcile the instructions into one authorized decision, then send equipment for sanitization.

Topic reference: NIST SP 800-88 Rev. 2; Section 4.3.1, lifecycle decision context; PDF page 29.

Answer:

Owner, evidence reference and follow up date:

MS-02

Is sanitization governed by an established policy?

Connect data sensitivity, acceptable methods, responsibilities, documentation and supplier assurance. The policy records why each sanitization process was selected, and the disposal receipt sits alongside that record.

Evidence to gather

Policy, approved methods, responsible owners and documentation requirements.

To complete the record

Complete the program decisions first, then evaluate individual disposal jobs.

Topic reference: NIST SP 800-88 Rev. 2; Sections 4.1 and 4.7; PDF page 27.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

MS-03

Have all storage components been identified?

A device often holds storage beyond its obvious drive. Include removable cards, embedded storage and other components that may hold target data. A vendor statement of volatility can help identify less visible storage.

Evidence to gather

Device/storage inventory, serial identifiers and vendor storage/volatility information.

To complete the record

Confirm the relevant storage with the vendor or a qualified examiner before selecting a technique.

Topic reference: NIST SP 800-88 Rev. 2; Section 4.3.1 and Appendix B; PDF page 30.

Answer:

Owner, evidence reference and follow up date:

MS-04

What data sensitivity and release conditions govern the decision?

Record the sensitivity of the information, whether media will be reused and whether it stays under organizational control. Those conditions influence the selected method and the assurance needed.

Evidence to gather

Data classification, intended destination, reuse decision and control/transfer conditions.

To complete the record

Have the information and asset owners approve the decision basis.

Topic reference: NIST SP 800-88 Rev. 2; Sections 4.3.2-4.3.6; PDF page 30.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

MS-05

Is the selected method suitable for the media and purpose?

Clear, purge and destroy describe different sanitization approaches. Choose an approved technique for the actual storage and risk. Verification and validation confirm the selected method met its objective, a step beyond formatting a volume, deleting files or making a device inoperable.

Evidence to gather

Selected method/technique, media specification and technical decision rationale.

To complete the record

Use approved media specific procedures.

Topic reference: NIST SP 800-88 Rev. 2; Sections 3.1 and 4.4; PDF page 17.

Answer:

Owner, evidence reference and follow up date:

MS-06

Can the supplier explain how the sanitization function works?

Assurance comes from documented media capabilities, limitations and implementation evidence, read alongside the product label or command name. Obtain that evidence so the organization can make an informed selection.

Evidence to gather

Vendor documentation, supported interfaces, assurances and approved tool/procedure records.

To complete the record

Obtain the outstanding technical details, then decide on a sanitization capability for sensitive data.

Topic reference: NIST SP 800-88 Rev. 2; Sections 4.1 and 4.3.1; Appendix B; PDF page 27.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

MS-07

If using cryptographic erase, were its prerequisites established?

Erasing a key addresses the data that key protects, under suitable cryptographic and storage conditions. Identify whether sensitive plaintext existed outside the protected scope and whether the implementation supports the intended operation.

Evidence to gather

Encryption history, protected data scope, key hierarchy and implementation assurance.

To complete the record

Have a qualified specialist confirm the prerequisites before cryptographic erase is accepted as a purge.

Topic reference: NIST SP 800-88 Rev. 2; Sections 3.2.1-3.2.4; PDF page 21.

Answer:

Owner, evidence reference and follow up date:

MS-08

Have all relevant key copies and recovery paths been considered?

Escrowed, backed up or externally managed keys are part of the recoverability question. Record the key relationships and how each relevant copy is handled, keeping key values out of the checklist.

Evidence to gather

Key lifecycle/escrow design, provider responsibilities and evidence of the authorized operation.

To complete the record

Locate every key copy and recovery path, then rely on cryptographic erase.

Topic reference: NIST SP 800-88 Rev. 2; Sections 3.2.3 and 3.2.5; PDF page 24.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

MS-09

Is the scope of partial or selective sanitization understood?

Data can also reside beyond the intended file, partition or logical boundary, including remapped or overprovisioned areas. A narrow operation needs a justified scope and assurance that relevant copies were addressed.

Evidence to gather

Target data scope, storage layout, known copies and technical limitations.

To complete the record

Have the storage owner or specialist evaluate the boundary before accepting a partial operation.

Topic reference: NIST SP 800-88 Rev. 2; Section 4.2; PDF page 28.

Answer:

Owner, evidence reference and follow up date:

MS-10

Do cloud and virtual storage arrangements provide adequate evidence?

The physical media often sit under the provider's control. Identify the provider's deletion, retention, key management and sanitization responsibilities and what the customer can verify for the selected service.

Evidence to gather

Service terms, retention/key controls, provider attestations and data copy inventory.

To complete the record

Clarify provider capabilities and remaining copies.

Topic reference: NIST SP 800-88 Rev. 2 FAQ (July 16, 2026), Question 13.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

MS-11

Was the operation verified for completion and anomalies?

Verification inspects the outcome of the technique used. Capture completion information, errors and relevant media or equipment conditions. A tool reporting success is one input to assurance, and validation makes the final suitability decision.

Evidence to gather

Tool/equipment identity and version, completion status, errors and inspection results.

To complete the record

Review unexpected results before releasing the media or accepting the job.

Topic reference: NIST SP 800-88 Rev. 2; Section 4.5.1; PDF page 33.

Answer:

Owner, evidence reference and follow up date:

MS-12

Was the outcome validated against the decision criteria?

Validation decides whether the result is sufficient for the target data and the organization's accepted risk. Validation also confirms that the method, scope and equipment suited the media.

Evidence to gather

Verification record, data sensitivity, acceptance decision and open concerns.

To complete the record

Escalate a result that falls short of the criteria and apply the approved follow up procedure.

Topic reference: NIST SP 800-88 Rev. 2; Section 4.5.2; PDF page 34.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

MS-13

Can each device be linked to an adequate sanitization record?

Retain identifying information, the selected method/technique, tool version, verification and validation details, people and dates. The document explains what was done to each identified device, item by item, beyond the collection of the batch.

Evidence to gather

Device linked certificates/records, method details, responsible people and disposition.

To complete the record

Identify every device and complete its record, then close the batch.

Topic reference: NIST SP 800-88 Rev. 2; Section 4.6 and Appendix C; PDF page 34.

Answer:

Owner, evidence reference and follow up date:

MS-14

Are the people, tools and disposal handoffs controlled?

Define competence, tool approval and provider responsibilities. Protect the media until the required operation and acceptance are complete, including transfer to an outside facility.

Evidence to gather

Training/authorization, equipment records, service agreements and transfer records.

To complete the record

Review the handoff with the asset owner and supplier and assign an owner to each open control.

Topic reference: NIST SP 800-88 Rev. 2; Sections 4.1, 4.3.4 and 4.7; PDF page 27.

Answer:

Owner, evidence reference and follow up date:

Web Addresses for the Sources Cited

1. NIST SP 800-88 Rev. 2; Section 4.3.1, lifecycle decision context; PDF page 29: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf#page=29

© 2026 Global Digital Forensics, Inc. All rights reserved.

2. NIST SP 800-88 Rev. 2; Sections 4.1 and 4.7; PDF page 27: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf#page=27
3. NIST SP 800-88 Rev. 2; Section 4.3.1 and Appendix B; PDF page 30: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf#page=30
4. NIST SP 800-88 Rev. 2; Sections 3.1 and 4.4; PDF page 17: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf#page=17
5. NIST SP 800-88 Rev. 2; Sections 3.2.1-3.2.4; PDF page 21: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf#page=21
6. NIST SP 800-88 Rev. 2; Sections 3.2.3 and 3.2.5; PDF page 24: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf#page=24
7. NIST SP 800-88 Rev. 2; Section 4.2; PDF page 28: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf#page=28
8. NIST SP 800-88 Rev. 2 FAQ (July 16, 2026), Question 13: https://csrc.nist.gov/files/pubs/sp/800/88/r2/final/docs/sp800-88r2-faq.pdf#page=8
9. NIST SP 800-88 Rev. 2; Section 4.5.1; PDF page 33: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf#page=33
10. NIST SP 800-88 Rev. 2; Section 4.5.2; PDF page 34: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf#page=34

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.