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.

Edition 2026-11-03 · Updated November 3, 2026 · miami-computer-forensics.com/guides/media-sanitization-checklist/

Baseline: NIST SP 800-88 Rev. 2, with July 2026 FAQ. Updated November 3, 2026.

Use the questions to prepare the review

Use this checklist to plan the decisions and records around sanitization; the erasure itself follows your approved, media specific procedure. Preserve material subject to a hold or other retention decision before any destructive work. Media specific techniques require approved procedures and qualified personnel.

For this media retirement decision, distinguish records you can locate from answers awaiting confirmation. Mark an answer verified once someone has checked the record behind it. Assign an owner to unresolved questions and explain exclusions.

Keep encryption keys and confidential device contents in their secured location, and keep preservation and disposal records with the authorized owner.

Use these media retirement decision questions to prepare the discussion. Each question cites the NIST section it comes from, so your team can check the source directly.

© 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 counsel requires material to be retained. Sanitization is irreversible in its intended result. Record this preservation decision in the GDF preparation workflow and link the applicable hold instructions.

Evidence to gather

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

If something is missing

Resolve conflicting or missing instructions before sending 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. A disposal receipt shows that custody changed hands; the sanitization record shows which method was chosen and why.

Evidence to gather

Policy, approved methods, responsible owners and documentation requirements.

If something is missing

Identify the missing decisions in the program before evaluating 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 may contain more than 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.

If something is missing

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.

If something is missing

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, rather than a format, a deletion or a broken device, shows that the selected method achieved its objective.

Evidence to gather

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

If something is missing

Use approved media specific procedures matched to each device.

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 rests on evidence about the media itself. Obtain the relevant media capabilities, constraints and implementation evidence so the organization can make an informed selection.

Evidence to gather

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

If something is missing

Ask for unresolved technical details before accepting 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 only addresses the data protected by that key 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.

If something is missing

Have a qualified specialist review the prerequisites for a cryptographic 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 can affect whether data remains recoverable. Record the key relationships and how the relevant copies are handled, keeping the key values in their secured store.

Evidence to gather

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

If something is missing

Confirm key locations and recovery paths before relying 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 a partial or selective sanitization understood?

Data can exist outside the intended file, partition or logical boundary, including remapped or overprovisioned areas. Give a narrow operation a justified scope and confirm that relevant copies were addressed.

Evidence to gather

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

If something is missing

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 customer may not control the physical media. Identify the provider's deletion, retention, key management and sanitization responsibilities and what can actually be verified for the selected service.

Evidence to gather

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

If something is missing

Clarify provider capabilities and remaining copies, and record the provider's own sanitization evidence for media it controls.

Topic reference: July 16, 2026 FAQ; Question 13; MEDIA88 section 4.2; PDF page 8.

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 the suitability decision rests on the full verification record.

Evidence to gather

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

If something is missing

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 fit the media.

Evidence to gather

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

If something is missing

Reject or escalate an inadequate result 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 record states what was done to each identified item of media, beyond confirming that a batch was collected.

Evidence to gather

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

If something is missing

Resolve unidentified media or incomplete records before considering the batch closed.

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.

If something is missing

Review the handoff with the asset owner and supplier and assign missing controls.

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:

Plan the Retirement With an Examiner

Bring the list of devices you plan to retire and the people who control retention decisions to a free consultation with a senior GDF examiner. On that first call we confirm what must be preserved before any destructive work, review the sanitization methods and verification records you plan to use, and set

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

out how we can help. Call (786) 219-1210 or the 24/7 hotline at (800) 868-8189, or write to info@evestigate.com. To keep preparing, browse the forensics guide library.

Talk to a Senior GDF Examiner

Bring this guide to a free consultation. We review your answers, identify what to preserve or test first and set out the work, the timeline and the deliverables.

Miami office: (786) 219-1210 · **24/7 hotline:** (800) 868-8189 · **Email:** info@evestigate.com

miami-computer-forensics.com

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