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 · Online at newyorkcomputerforensics.com/guides/media-sanitization-checklist/

Use the questions to prepare the review

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 still to be confirmed. Assign an owner to each open question and explain exclusions.

Keep preservation and disposal records with the authorized owner.

MS-01

Has the owner authorized disposition and checked retention needs?

Confirm what may be erased or destroyed and whether the business or a legal hold requires material to be retained. Sanitization is irreversible in its intended result.

Evidence to gather

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

To complete this item

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. Pair each disposal receipt with the record of the sanitization process selected.

Evidence to gather

Policy, approved methods, responsible owners and documentation requirements.

To complete this item

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.

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

Answer:

Owner, evidence reference and follow up date:

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.

To complete this item

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 this item

Have the information and asset owners approve the decision basis.

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

Answer:

Owner, evidence reference and follow up date:

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. Verify for each device that the selected method achieved its objective.

Evidence to gather

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

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

To complete this item

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?

Obtain the relevant media capabilities, limitations and implementation evidence so the organization can make an informed selection.

Evidence to gather

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

To complete this item

Ask for the remaining 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:

MS-07

If using cryptographic erase, were its prerequisites established?

Cryptographic erase covers 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.

To complete this item

Have a qualified specialist review the prerequisites rather than treating encryption enabled as proof of successful purge.

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

Answer:

Owner, evidence reference and follow up date:

MS-08

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

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.

Evidence to gather

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

To complete this item

Resolve unknown key locations or 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:

MS-09

Is the scope of partial or selective sanitization understood?

Data can exist outside 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 conditions.

To complete this item

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?

In a cloud or managed service, the provider holds 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.

To complete this item

Clarify provider capabilities and remaining copies, and describe disposal of provider media in the provider's own terms.

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

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

Answer:

Owner, evidence reference and follow up date:

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's success report is one input to assurance, alongside verification of the outcome.

Evidence to gather

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

To complete this item

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. Confirm that the method, scope and equipment suit the media, alongside the completion record.

Evidence to gather

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

To complete this item

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:

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 medium.

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

Evidence to gather

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

To complete this item

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.

To complete this item

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:

All five checklists are also in one editable workbook: GDF Standards Readiness Checklists (XLSX).

Get a Free Consultation

The first call is a free consultation with a senior examiner. We review the matter, the evidence and the deadline, and outline the collection and analysis it needs. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.