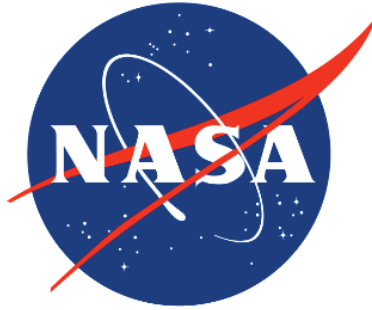




Information Technology Security Handbook

Media Protection and Sanitization

February 2023

Version 2.3

OFFICE OF THE CHIEF INFORMATION OFFICER

CYBERSECURITY AND PRIVACY DIVISION

Document Properties

- **Maintained by:** OCIO CSPD Team
- **Filename:** ITS-HBK-2810.11-2C Media Protection and Sanitization
- **Supersedes:**
 - Version 2.2

Table 1: Revision History

Version	Date	Change Description
1.0	07/13/2012	ITS-SOP-0035, Digital Media Sanitization was replaced by the updates made within this Handbook.
1.1	6/24/2015	Reviewed, updated, and signed by SAISO .
1.2A	3/9/2018	<ul style="list-style-type: none"> • Revised to comply with new formatting standards • Some material transferred to ITS-HBK 2810.11-01A, Media Protection.
1.3	7/10/2018	ITS-HBK-2810.01A consolidated with ITS-HBK-2810.11-02A, Media Protection and circulated for CISO community review and comment.
2.0	6/5/2019	<ul style="list-style-type: none"> • Updated and consolidated handbook submitted for SAISO review and approval. • Once approved, earlier versions of Media Protection and Digital Media Sanitization will be removed from NODIS and the updated/consolidated version will be posted with new effective date.
2.1	5/24/2021	Removed statement from Appendix C about relating non-NASA removable media or NASA media in a partner's computing to a business need; added reference to ODVs being maintained by CSET.
2.2	09/30/2021	Updated to reflect SP 800-53 Rev. 5 and new CUI policy.
2.3	02/14/2023	Annual update.

Table of Contents

1. Introduction	1
1.1 Purpose	1
1.2 Scope	2
1.3. Point of Contact(s)	4
1.4 Applicability	4
1.5 Applicable Documents	4
2. Security Controls and Corresponding Roles and Responsibilities.....	5
3. Confidentiality and Sensitivity Definitions	17
4. Determining Confidentiality and Sensitivity of Information	18
4.1 Establishing the Confidentiality Level of a System	20
4.2 User-Based Sensitivity/Confidentiality Determination	21
4.3 Special Considerations	22
5. Tagging Media Based on Confidentiality and Sensitivity Ratings	22
6. Digital Media Sanitization Considerations	24
7. Digital Media Sanitization Specifics	25
7.1 Approved Sanitization Tools	26
7.1.1 Digital Media Sanitization Tools	26
7.2 Recording and Verifying Sanitization	27
7.3 Records Retention Compliance	27
8. Sanitization Instructions for Media Types	27
8.1 Media Documentation and Sorting	29
8.2 Inoperable Media Sanitization	29
8.3 General Media Sanitization	31
8.4 Special Case Media Sanitization	33
8.5 Media Sanitization Requirements Based on Confidentiality and Sensitivity	35
9. Digital Media Inspection and Verification (Sampling)	44
9.1 Digital Media Inspection and Verification Workflow	45
9.2 Frequency of Inspection and Verification	48
9.3 Sample Selection	48
9.4 Samples and Rejection Limits	50

9.5 Verification Testing Requirements	50
10. Digital Media Destruction Process	65
11. Exceptions to Media Sanitization Procedures.....	67
Appendix A: Examples of Information Appropriate for Public Release	68
Appendix B: Examples of Information Not Appropriate for Public Release	70
Appendix C: Media Use Policy	73
Appendix D: Media Sanitization Record Template	74
Appendix E: Acronyms	76
Appendix F: Definitions.....	78
Figure 1: Media Confidentiality Sensitivity Determination Criteria	18
Figure 2: Media Confidentiality, Sensitivity, and Disposition Workflows	20
Figure 3: Inoperable Media Sanitization Workflow	30
Figure 4: General Media Sanitization Workflow	32
Figure 5: Special Case Media Sanitization Workflow	34
Figure 6: NASA Inspection and Verification Workflow	45
Figure 7: Media Destruction Workflow	65
Table 1: Approved Media Sanitization Tools	26
Table 2: Media Sanitization Requirements based on Confidentiality or Sensitivity	36
Table 3: Good, Better, Best Approach to Selecting and Sampling Method	49
Table 4: 90% Confidence Level Lot/Batch Sizes, Sample Sizes, & Rejection Limits	50

This page intentionally left blank

Distribution:

CSET



Associate Chief Information Officer for
Cybersecurity & Privacy

1. Introduction

NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*). NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, *Security of Information and Information Systems*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53 Rev.5*.

NPR 2810.1 designates this Handbook as a guide of NASA's Media Protection (MP) information security controls. This Handbook also establishes NASA policy for ensuring digital media sanitization and the associated process to ensure that improper sanitization or destruction of digital media is not the source of an unapproved leakage of non-public information held by NASA, NASA contractors, and/or NASA partners. This Handbook has been written to satisfy the guidance and best practices of *NIST SP 800-88: Guidelines for Media Sanitization*. The content of this document, in conjunction with NPD/R 2810.1, defines NASA policy and procedures to address MP-1

This Handbook supports implementation of requirements in NPR 2810.1 and NPD 2810.1. It also augments NIST guidance with NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated. The Agency's organizationally defined values are integrated into the control requirements within RSA ARCHER in the Risk Information Security Compliance System (RISCS).

1.1 Purpose

The Media Protection control family relates to the secure use of information storage media. Storage media can take one of two forms – digital or non-digital. Non-digital media typically consists of paper, film, microfilm, microfiche, etc. Digital media is comprised of mobile computing devices, laptops, Personal Digital Assistants (PDAs), "smart phones," and removable storage devices such as USB drives, flash drives, writeable CDs and DVDs, memory cards, external hard drives, storage cards, diskettes, magnetic tapes, external/removable hard drives, or any electronic device that can be used to copy, save, store and/or move data from one system to another.

The objective of the control family is to prevent or mitigate data loss and/or unauthorized access to NASA information and information systems, due to a failure to secure media, or a failure to sanitize media prior to reuse or disposal.

This Handbook presents a comprehensive framework for all aspects of digital media protection. The processes and workflows in this Handbook, if followed properly, will allow NASA to assert to a specific level of confidence that NASA data is being properly handled, marked, stored, and sanitized.

The Handbook outlines processes associated with sanitization to ensure that improper sanitization, or improper destruction, of digital media is not the source of an unapproved leakage of non-public information held by NASA, NASA contractors, and/or NASA partners. It also presents decision processes which address what to do when, or if, the sanitization processes break down or fail.

Further, this Handbook provides the guidelines and best practices for Information System Owners (ISOs), Information Security personnel, and Property Disposal personnel – whether they are NASA employees, NASA contractors, or NASA partners – to ensure that the requirements to protect NASA information via handling the sanitization of digital media are consistent.

Additionally, this Handbook meets and exceeds the guidelines outlined in the National Institute of Standards and Technology Special Publication *NIST SP 800-88: Guidelines for Media Sanitization*.

All government and non-government personnel shall follow these procedures from purchase to disposal for all NASA information that is stored on digital media under their control regardless of whether such media have been connected to NASA networks.

This document also establishes the requirements and best practices for NASA contractors whose contracts, information technology devices, and/or systems include the collection, processing, storing, displaying, disseminating, or transmitting of NASA information.

- For any NASA information or information systems, the contractor is responsible for implementing and complying with the requirements of this Handbook within the overall context of NASA information technology security program policy.
- The Prime NASA contractor is responsible for passing down these media sanitization requirements both for contractor-owned equipment and for subcontractors at any tier to the extent necessary to ensure compliance.

1.2 Scope

The provisions of this Handbook apply to all media on NASA-owned computing devices (including mobile devices) and removable media/storage containers.¹ The Handbook includes *NIST SP 800-53 Rev.5*

¹ While media protection and sanitization for partner-owned devices are out of scope for this Handbook, partners are required to securely handle and dispose of media containing NASA data according to the terms of their organization's agreement with the Agency.

controls for media handling and instructions for determining the sensitivity level and labelling requirements for media.

Note that national security information is not within the scope of this Handbook. This

Handbook specifically provides the following:

- Controls for media access, marking, storage, transport, sanitization, and use;
- Instructions and processes for sanitization of digital media;
- Instructions and processes for inspecting and verifying to a level of 90% confidence that digital media is properly sanitized;
- A statistically valid sampling methodology to ensure that NASA digital media is properly sanitized;
- Frequency of sampling to satisfy the NASA's acceptable risk level for excess equipment;
- Specific instructions and processes for destruction of digital media;
- A requirement that Centers and contractors identify responsible officials and to ensure record keeping on all sanitized digital media;
- A requirement that Centers and contractors secure NASA's digital media during all facets of the digital media sanitization process; and
- A process to address potential failures that may occur during digital media sanitization.

Contractor managers or ISOs may specify and implement additional requirements to address specific risks, vulnerabilities, or threats within a particular operating unit and/or system as long as the justification for such additional requirements is documented and retained for as long as such requirements are in place.

The Agency Chief Information Officer (CIO) and Senior Agency Information Security Officer (SAISO) have authorized the Cybersecurity Standards and Engineering Team (CSET) via the Agency Security Configuration Standards (ASCS) initiative to create binding Specifications and Technical Standards related to Agency cybersecurity topics.

The NASA Technical Standards Program (NTSP), sponsored by the Office of the NASA Chief Engineer, recognizes CSET as a standards-developing organization within the Agency.

IT Handbooks, IT Security Handbooks, and NASA IT Requirements are issued by the Office of the Chief Information Officer (OCIO) and provide specific requirements to protect the confidentiality, integrity, and availability of NASA information and information systems. Pursuant to NASA Procedural Requirements (NPR) 1400.1H, NASA Directives and Charters Procedural Requirements, Appendix D, these documents work in conjunction with NASA Policy Directives (NPDs) and NPRs by providing specific requirements to comply with relevant NPDs and NPRs governing NASA information and information systems. Handbooks are effective until formally cancelled, rescinded, or superseded by an updated document.

All NASA information and NASA information systems shall be managed in compliance with the requirements of CSET Specifications, CSET Technical Standards, IT Handbooks, IT Security Handbooks, and NASA IT Requirements in order to be authorized for use. Where necessary, information or information system owners, and program or project managers shall incorporate the requirements of CSET

Specifications, CSET Technical Standards, IT Handbooks, IT Security Handbooks, and NASA IT Requirements into contracts and program or other agency documents to ensure that these requirements are followed.

All of these documents including handbooks, specifications and standards are available at:

<https://cset.nasa.gov/ascs/>

This Handbook and the procedural guidance contained within remains in full force and effect until such time that the Handbook is formally cancelled, rescinded, or superseded by an updated document.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request for deviation from the procedural guidance set forth in this Handbook to support such decision. The documented rationale/justification shall be provided to the NASA Cyber Security and Privacy Division (CSPD) and the point of contact for this Handbook, in coordination with Center Information Security Officers (CISO), to review and validate for the record.

1.3. Point of Contact(s)

For any questions or comments regarding the contents of this Handbook, contact:

- hq-dl-cspd-policy@mail.nasa.gov

Any questions or concerns regarding perceived gaps in policy or implementation guidance, conflicting procedural requirements, lack of clarity pertaining to specified roles and responsibilities, or issues associated with interpretation shall be elevated to the NASA CSPD, in coordination with the CISO, and directed to the attention of the point of contact for this particular Handbook to address and resolve.

1.4 Applicability

This Handbook is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to Jet Propulsion Laboratory, a Federally Funded Research and Development Center (FFRDC), other contractors, authorized users, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

1.5 Applicable Documents

Federal Law

Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1896

- Freedom of Information Act (FOIA), 5 U.S.C. § 552, 1966

- The National Aeronautics and Space Act of 1958, Pub.L. 85-568, 72 Stat. 426
- Trade Secrets Act, 18 U.S.C 1905

Federal Information Processing Standards (FIPS)

FIPS 199, Standards for Security Categorization for Federal Information and Information Systems

- *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*

National Institute of Standards and Technology (NIST)

- *NPR 1600.2, NASA Classified National Security Information (CNSI)*
- *NIST SP 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations*
- *NIST SP 800-88, Guidelines for Media Sanitization*
- *NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices*

National Aeronautics and Space Administration (NASA)

- *NPR 2810.7, Controlled Unclassified Information*
- *NPD 1382.17, NASA Privacy Policy*
- *NPD 2540.1 Personal Use of Government Office Equipment Including Information Technology*
- *NPD 2810.1, NASA Information Security Policy*
- *NPR 1441.1, NASA Records Retention Schedules*
- *NPR 1382.1, NASA Privacy Procedural Requirements*
- *NPR 1600.1, NASA Security Program Procedural Requirements*
- *NPR 1600.2, Classified National Security Information (CNSI)*
- *NPR 2200.2, Requirements for Documentation, Approval and Dissemination of Scientific and Technical Information*
- *NPR 2810.1, Security of Information and Information Systems*
- *NPR 2841.1, Identity, Credential, and Access Management*

Cancellations, Updates, and Consolidations

- *ITS-HBK-2810.11-01, Media Protection*
- *ITS-HBK-2810.11-02, Digital Media Sanitization*

2. Security Controls and Corresponding Roles and Responsibilities

Agency-Wide

- *NASA Chief Information Officer (CIO)*
 - **Controls:** None
 - **Processes:** None
 - **Responsibilities:**

- Establishes NASA policy and standards with respect to digital media sanitization, digital media destruction, and inspection and verification efforts thereof.
- Approves the physical tools and software packages which are permissible for NASA to use for digital media sanitization.
- Approves, only with the concurrence of the Assistant Administrator for the Office of Strategic Infrastructure, any deviation of assignment of responsibilities with respect to the policies, procedures, and roles and responsibilities as outlined in this Handbook.
- In consultation with the Center Chief Information Officer (Center CIO), the Center
 - Chief Information Security Officer (Center CISO), and the Property Disposal Officer (PDO), allows for a flexible and cost-effective approach to the closeout of a large project or program where many digital media assets are assessed to be, or deemed to be, at the end-of-life. However, this approach must be conducted in a manner that assures that such media assets will not become the source of leakage of non-public information held by NASA and NASA contractors and/or NASA partners.
- Assistant Administrator for the Office of Strategic Infrastructure (AAOSI)
 - **Controls:** None
 - **Processes:** None
 - **Responsibilities:**
 - Approves, only with the concurrence of the NASA CIO, any deviation of assignment of responsibilities with respect to the policies, procedures, and roles and responsibilities as outlined in this Handbook.

Center Level

- *Center Chief Information Officer (CIO)*
 - **Controls:** None
- ○ **Processes:**
 - Approved Sanitization Tools (Section 7.1)
 - Media Sanitization Requirements (8.5)
- **Responsibilities:**
 - Ensures all Center personnel comply with the requirements of this Handbook.
 - Designates in writing which person or persons are responsible for the sanitization, verification, and disposition process under their jurisdiction, and shall maintain and update this record as necessary so that it will be available for the Office of Inspector General (OIG) or other lawful review and maintained in accordance with NASA's Record Retention Policy.
 - Ensures that inspection and verification of digital media sanitization is conducted in accordance with the policies and procedures outlined in this Handbook.
 - At a minimum, annually verifies that the personnel conducting sanitization of digital media have been appropriately trained in the use of authorized sanitization tools.

- Center Chief Information Security Officer (CISO)
 - **Controls:** None
 - **Processes:**
 - Digital Media Inspection and Verification Workflow (Section 9.1)
 - Digital Media Destruction Process (Section 10)
 - **Responsibilities:**
 - Ensures that Agency-approved sanitization tools are:
 - Used by all NASA and NASA contractor personnel responsible for digital media sanitization, and
 - Properly configured and functioning.
 - Ensures that inspection and verification of digital media sanitization is conducted in accordance with the policies and procedures outlined in this Handbook.
 - Routinely² tests the Center sanitization equipment and procedures to ensure they are performing as intended and as required by this Handbook.
 - Reviews NASA IT devices returning from international travel and ensure all required mitigation actions (currently scanning, wiping, and re-imaging the hard drive or mobile device to a known good state) are taken prior to authorizing the re-connection of the NASA IT devices directly within the Trusted Internet Connection boundary.
 - Verifies at least annually that the personnel conducting sanitization of digital media have been appropriately trained in the use of authorized sanitization tools.
 - Advises the Contracting Officer (CO) and/or Contracting Officer Technical Representative (COTR) on the proper tagging of digital media devices according to the level of Confidentiality or Sensitivity of the NASA information the device did, does, or will contain.
 - Verifies and ensures that the integrity of the digital sanitization process is meeting the minimum NASA sanitization and inspection and verification standards as set by the the NASA CIO.³
 - Ensures the security of digital media during the disposition process is adequate to assure such media will not become the source of leakage of non-public information held by NASA and NASA contractors and/or NASA partners.

² *NIST SP 800-88* states: “[Organizations] are expected to continually monitor and validate the effectiveness of their selected sanitization tools as they are used.” Therefore, as a best practice, persons acting in this capacity shall perform this task at least once per year but are encouraged to perform it on a more frequent basis and in accordance with a risk-based approach to security that is in alignment with the Agency’s approach to Continuous Monitoring.

³ If any part of the media sanitization process covered by this Handbook is being conducted by a contractor, off-Center, on devices that contain NASA data, the contract personnel shall contact the Contract Manager in lieu of the Center CISO when notified of any inconsistency, error, or failure of the media sanitization process. The Contract Manager shall, when notified, seek and follow the direction of the Center CISO, via the COTR, to resolve the inconsistency, error, or failure and ensure that NASA data is protected.

- When notified of a batch failure during the inspection and verification process, directs the Center PDO, the Media Inspection and Verification Personnel (MIVP), and if needed the COTR and the Contract Manager to properly and securely dispose of the rejected digital media in a manner which ensures that the information it does or may contain, will not become the source of a leakage of non-public information held by NASA, NASA contractors, and/or NASA partners.
- Enforces NASA policy and standards with respect to the efforts of digital media sanitization, inspection, and verification.
- Ensures that documentation of inspection and verification results are maintained in accordance with NASA's Record Retention Policy.
- In consultation with the NASA CIO, the Center CIO, and the PDO, allows for a flexible and cost-effective approach to the closeout of a large project or program, such as the retirement of the Space Shuttle program, where many digital media assets are assessed to be, or deemed to be, at the end-of-life. However, this approach must be conducted in a manner that assures that such media assets will not become the source of leakage of non-public information held by NASA and NASA contractors and partners.

Agency Privacy Manager (APM)

- **Controls:** None
- **Processes:** None
- **Responsibilities:**
 - Advises the CO and/or COTR on the proper tagging of devices that may have privacy related material on them, according to the level of Confidentiality or Sensitivity of the NASA information the device did, does, or will contain.
- *Contracting Officer (CO)*
 - **Controls:** None
 - **Processes:** None
 - **Responsibilities:**
 - Ensures that all non-government owned computers are handled in accordance with the terms and conditions of the NASA contract that governs their use, if such contracts contain different requirements than are contained in this Handbook.⁴⁴
 - Includes the NASA contractor responsibilities set out in this document as a requirement and best practice in all NASA contracts that include IT support or resources.
- *Contracting Officer Representative (COR)*
 - **Controls:** None
 - **Processes:** None
 - **Responsibilities:**

⁴ This responsibility may be delegated to the COTR, at the discretion of the CO.

- If delegated the responsibility from the CO, ensures that all non-government owned computers are handled in accordance with the terms and conditions of the NASA contract that governs their use, if such contracts contain different requirements than are contained in this Handbook.
- In coordination with the CISO, ensures the security of contractor-owned digital media during the disposition process is adequate to assure such media will not become the source of leakage of non-public information held by NASA, NASA contractors and/or NASA partners.
- Routinely tests the contractors' sanitization equipment and procedures to ensure they are performing as intended and as required by their contract and/or this Handbook.
- Verifies at least annually that contractor personnel conducting sanitization of digital media have been appropriately trained in the use of authorized sanitization tools.
- Seeks and follows the direction of the Center CISO when notified of any inconsistency, error, or failure of the media sanitization process, to ensure that NASA data does, or will not become the source of a leakage of non-public information held by NASA, NASA contractors, and/or NASA partners.
- *Center Export Control Administrator* ○
 - Controls:** None
 - **Processes:** None
 - **Responsibilities:**
 - Ensures that Export Control (e.g., International Traffic in Arms Regulations (ITAR)/ Export Administration Regulation (EAR)) information in electronic form is properly labeled on digital media.
 - Advises the CO and/or COR on the proper tagging of devices according to the level of Confidentiality or Sensitivity of the information the device did, does, or will contain.
- *Contract Manager*
 - **Controls:** None
 - **Processes:** Digital Media Destruction Process (Section 10)
 - **Responsibilities:**
 - Ensures that any NASA information contained on any external information system associated with their contract (including sub-contractor systems) complies with the requirements of this Handbook.
 - Ensures that all non-government-owned computers are handled in accordance with the terms and conditions of the NASA contract that governs their use, if such contracts contain different requirements than are contained in this Handbook.
 - Designates in writing which person or persons are responsible for sanitization, verification, and disposition process under their jurisdiction, and shall maintain and update this record as necessary so that it will be available for the OIG or other lawful review.

- Ensures the tagging of contractor-owned devices according to the level of Confidentiality, Sensitivity, and Personnel categorization of the information the device did, does, or will contain.
 - Is responsible for the physical security of devices, and the information they contain, which are turned over to them or their organization prior to disposition actions requiring digital media sanitization.
 - Ensures the security of digital media during the disposition process is adequate to assure such media will not become the source of unapproved leakage of non-public information held by NASA, NASA contractors, and/or NASA partners.
 - Routinely tests their sanitization equipment and procedures to ensure they are performing as intended and as required by their contract and/or this Handbook.
 - Verifies at least annually that the personnel conducting sanitization of digital media have been appropriately trained in the use of authorized sanitization tools.
 - Seeks and follows the direction of the Center CISO when notified of any inconsistency, error, or failure of the media sanitization process, to ensure that NASA data does not/will not become the source of a leakage of non-public information held by NASA, NASA contractors, and/or NASA partners.
 - Specifies and implements additional requirements to address specific risks, vulnerabilities, or threats within its operating unit/systems as long as the justification for such additional requirements is documented and retained for as long as such requirements are in place.
 - Designates in writing which person(s) is/are responsible for each step of the local sanitization, verification, and disposition process under their jurisdiction, and maintain and update this record as necessary so that it will be available for OIG or other lawful review.
- *Media Inspection and Verification*
 - Personnel (MIVP) ○ **Controls:** None
 - **Processes:** Digital Media Inspection and Verification Workflow (Section 8.1)
 - **Responsibilities:**
 - Ensures that the digital media sanitization process is executed properly utilizing the inspection and verifications workflow process and the Sanitization Verification Testing Requirements listed in Table 5 of Section 8.5.
 - Ensures records documenting sanitization and verification of digital media are properly recorded and associated to the proper asset.
 - Ensures that the responsible Center PDO and/or Center CISO are properly informed of any instances of media sanitization failure and when the failure rates exceed those rates which are established by this Handbook.
 - Ensures the security of digital media during the inspection and verification process is adequate to assure such media, and the information it may contain, will not become the source of a leakage of non-public information held by NASA, NASA contractors, and/or NASA partners.

- Routinely tests the Center sanitization equipment and procedures to ensure they are performing as intended and as required by this Handbook.
- Utilizes a selection methodology that is appropriate to the sample size and conforms to the standards for inspection and verification as outlined in this Handbook.
- Documents the sampling methodology followed for each sampled batch, and record the results thereof for review by the Center CISO if needed.
- When the inspection and verification process results in a failure, after the responsible Center PDO and/or Center CISO are properly informed, proceeds at the direction of the Center PDO and/or the Center CISO to properly and securely dispose of the digital media in a manner which ensures that the information it does or may contain, will not become the source of a leakage of non-public information held by NASA, NASA contractors, and/or NASA partners.
- *Media Sanitization Personnel (MSP)* ○
 - Controls:** None
 - **Processes:**
 - Media Documentation and Sorting (Section 8.1)
 - General Media Sanitization (Section 8.3)
 - Special Case Media Sanitization (Section 8.4)
 - Digital Media Destruction Process (Section 10)
 - **Responsibilities:**
 - Ensures the security of digital media during the sanitization process is adequate to assure such media, and the information it does or may contain, will not become the source of a leakage of non-public information held by NASA, NASA contractors, and/or NASA partners.
 - Ensures records documenting sanitization and verification of digital media are properly recorded and associated with the proper asset.
 - Ensures the Media Sanitization Record Template (found in Appendix D), or electronic equivalent record, has been completed prior to any digital media being sanitized.
 - Routinely tests the Center sanitization equipment and procedures to ensure they
 - are performing as intended and as required by this Handbook.
- *Property Disposal Officer (PDO)*
 - **Controls:** None
 - **Processes:**
 - Digital Media Sanitization Considerations (Section 6)
 - Sanitization Instructions for Media Types (Section 8)
 - **Responsibilities:**
 - Designates in writing which person is, or which persons are, responsible for each step of the local sanitization, verification, and disposition process under their jurisdiction, and maintains and updates this record as necessary so that it will be available for OIG or other lawful review.

- Is responsible for the physical security of devices and the information they may contain, which are turned over to them or their organization prior to disposition actions requiring digital media sanitization.
- Ensures the security of digital media during the disposition process is adequate to assure such media will not become the source of leakage of non-public information held by NASA, NASA contractors, and/or NASA partners.
- Ensures the final check of records documenting proper sanitization and verification of digital media has been conducted before final disposition takes place.
- Prior to sanitization, confirms that any Media Confidentiality and Sensitivity Tags remain on the digital media device.
- Ensures, after sanitization has been completed and verified, that the Media Confidentiality and Sensitivity Tags have been properly removed only on digital media devices which are to leave the control of NASA.
- Ensures that MSP are routinely testing their sanitization equipment and procedures to ensure they are performing as intended and as required by this Handbook. When notified of a batch failure during the inspection and verification process, consults with and follow the direction of the Center CISO to properly and securely dispose of the rejected digital media in a manner which ensures that the information it does or may contain, will not become the source of a leakage of non- public information held by NASA, NASA contractors, and/or NASA partners.
- In consultation with the NASA CIO, the Center CIO, and the Center CISO, allows for a flexible and cost-effective approach to the closeout of a large project or program, such as the retirement of the Space Shuttle program, where a large number of digital media assets are assessed to be, or deemed to be, at the end-of-life. However, this approach must be conducted in a manner that assures that such media assets will not become the source of leakage of non-public information held by NASA, NASA contractors, and/or NASA partners.

Information System Level

- *Information System Owner (ISO)*
 - **Controls:** MP-2: Media Access; MP-3: Media Marking; MP-4: Media Storage; MP-5: Media Transport; MP-6: Media Sanitization ○

Processes:

- Determining Confidentiality and Sensitivity of Information (Section 4)
- Specialized Considerations (Section 4.3)
- Sensitivity Determination Workflow (Section 7.4)
- Sanitization Instructions for Media Types (Section 8)
- Media Documentation and Sorting (Section 8.1),
- Inoperable Media Sanitization (Section 8.2)

- General Media Sanitization (Section 8.3)
- Special Case Media Sanitization (Section 8.4)
- Digital Media Inspection and Verification Workflow (Section 9.1)

o **Responsibilities:**

- Ensures access to digital and non-digital media containing non-public NASA information is restricted to authorized individuals.
- Ensures that all NASA information made available on media to the public at large is in accordance with the requirements of existing laws, applicable policies, and the requirements of the Office of Communication.
- Analyzes all documents planned for publication against the tables in Appendices A and B to ensure that no inappropriate content is disseminated.
- Ensures media for information system operations, digital and non-digital, are marked appropriately in a manner consistent with organizationally defined values.
- Maintains both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, compact disks, digital video disks, and portable computing devices) and non-digital media (e.g., paper, microfilm) related to the information system.
- Ensures markings include applicable indications of intended distribution and/or handling requirements (e.g., Controlled Unclassified Information (CUI)).
- Ensures media used for NASA information system operation and restoration (e.g., backups, procedure manuals) is physically protected and securely stored in a controlled area.
- Ensures media storage in controlled facilities is stored in an area accessible only to designated individuals and/or in a locked container.
- Ensures, if stored media uses Data at Rest (DAR) encryption:
 - The strength of the cryptographic mechanisms is commensurate with the classification and sensitivity of the information;
 - Establish and maintain cryptographic key management that provides the required protection and ensures the availability of the information in the event of cryptographic key loss by users; and
 - Destruction of stored media is in accordance with this Handbook and *NIST SP 800-88*.
- Ensures backup copies of operating system and other critical information system software is stored in fire-rated containers that are not co-located with the operational software.
- Ensures information system media that are transported outside the area of a NASA controlled facility are:
 - Encrypted in accordance with NASA policy and procedures using validated encryption solutions for digital media;
 - Stored in locked containers;

- Handled only by custodians/couriers approved by the ISO, mail, or an ISO approved commercial transport or delivery service with an accountable tracking system and manifest included in shipment; and
 - Documented in a formal log identifying the media, custodian, the time it was provided to the custodian, and destination.
 - Designates the custodian/courier that is authorized to provide the media transport.
 - Ensures adherence to media sanitization requirements in accordance with this Handbook and NIST SP 800-88.
 - Ensures non-digital sensitive information (e.g., CUI) media is sanitized/disposed of in accordance with this Handbook, NIST SP 800-88, and NPR 2810.7.
 - Ensures a record of media sanitization is maintained using the “Media Sanitization Record Template” in Appendix D.
 - Ensures all portable/removable storage media are sanitized in a manner consistent with organizationally defined values.
 - Ensures media with federal records are not sanitized/disposed of unless in compliance with NPR 1441.1.
 - Designates, in consultation with the Information Owner (IO), the Confidentiality, Sensitivity, and Personnel categorization of information on any digital media.
 - Ensures that export control (e.g., ITAR/EAR) and/or Privacy information in electronic form is/are properly labeled.
 - Advises the CO and/or COTR on the proper tagging of devices according to the level of Confidentiality or Sensitivity of the information the device did, does, or will contain.
 - Initiates the use of the Media Sanitization Record Template (found in Appendix D) on systems, or media, that are removed for sanitization, replacement, or are re- purposed outside of the ISO’s control.
 - Advises the Center CISO and MSP of the highest level of information Sensitivity/Confidentiality on the device to be sanitized.
 - Is responsible for implementing and complying with the requirements of this Media Sanitization Handbook for any NASA information or information systems within the overall context of NASA information technology security program policy.
- *Information System Security Officer (ISSO)*
 - **Controls:** None
 - **Processes:** None
 - **Responsibilities:**
 - Advises the ISO of the highest level of information sensitivity/confidentiality on the device to be sanitized.
 - *Information Owner (IO)*
 - **Controls:** MP-7: Media Use
 - **Processes:** None

- **The IO:**

- Works with the ISO to classify information and media and develop guidelines for handling the information/media.
- Develops alternative guidance as outlined above in the following circumstances:
 - The information system does not comply with agency policy or meet the Agency-level Organizationally Defined Values (ODVs) for the following controls:
 - SI-03: Malicious Code Protection
 - CM-06: Configuration Settings
 - SI-02: Flaw Remediation
 - SC-28(1): Protection of Information at Rest | Cryptographic Protection
- Ensures that users with a business need for removable media are provided with appropriate encryption mechanisms for protecting any sensitive data stored on the removable media
- Ensures that users of their information system who are at significant risk of advanced, targeted attacks (e.g., the Administrator, Counter-Intelligence staff) are identified and appropriate security measures are taken to address their unique risks (e.g., provide additional usage guidelines, implement additional compensating controls)
- Makes the final determination when there is ambiguity over the classification of removable media (e.g., whether a device was purchased “on behalf of NASA” or whether another organization is a formal NASA partner).
- Jointly develops alternate ODVs⁵ for this Media Use control (including the Media Use Policy) to apply to information managed by the information owner and an information system owned by the ISO. Such alternative ODVs shall:
 - Be documented in the system’s System Security Plan (SSP).
 - Be supported by a formal risk assessment conducted according to the guidance in the RA-3 Risk Assessment control found in NIST SP 800-53 Rev.5. The risk assessment should consider the risk to the information as well as the information system, with any residual risk accepted by the Authorizing Official (AO) for the information system.
- Provides, at minimum, the capability to:
 - Ensure that the loss of devices will be discovered and reported as per the Agency’s incident response process in a timely manner;
 - Maintain a reasonable awareness of the nature of the information stored on removable media so that the data loss can be properly characterized in the event of a lost or stolen device;
 - Counteract malware which may use removable media to spread;

⁵ Organizationally defined values (ODVs) are managed by the Cybersecurity Standards and Engineering Team (CSET). They are published at <https://cset.nasa.gov> under the specification name NASA-SPEC-2661. Where any ODVs in this handbook are different than the ODVs published by CSET, the CSET ODVs shall take precedence.

- Ensure that sensitive information on lost or stolen devices is protected; and
 - Ensure that each removable media device is under the responsibility of an ISO.
- Ensures the implementation of appropriate compensating controls, such as data loss prevention, physical security, mandatory encryption, and secure deletion/media sanitization:
 - Be clearly communicated to applicable users, with recorded user acknowledgement and periodic training.
 - Be documented in the security plan of the information system.
 - Remain consistent with all other applicable policies (e.g., NPR 2810.7, NPD 2540.1, and other Handbooks).
- *NASA User*
 - **Controls:** MP-7: Media Use
 - **Processes:**
 - Sanitization Instructions for Media Types (Section 8)
 - Digital Media Inspection and Verification Workflow (Section 9.1)
 - **Responsibilities:**
 - Follows the procedures and processes outlined in this Handbook from the creation through the disposal of all NASA information that is stored on digital media under their control regardless of whether such media have been connected to NASA networks.
 - Ensures compliance with NASA Federal Records retention requirements as outlined in NPR 1441.1.
 - Should not remove the Media Confidentiality and Sensitivity Tags on any digital media devices, but may remove, in preparation for sanitization, any other such tags which might contain NASA organizational identification, status labels, markings, device location, or activity log information, etc.
 - Complies with the agency's Media Use Policy, and/or other applicable policy that has been communicated to and acknowledged by the user.
 - Reports any suspicious or suspect media (such as devices with no identifiable owner or devices which have been used on unsafe computers like hotel kiosks) to the NASA Security Operations Center (SOC) immediately.
 - Reports all lost or stolen devices to the NASA SOC immediately.
 - Keeps track of their removable devices and the data stored on them. No specific inventory mechanism is prescribed, but the user must be able to recognize that a device has been lost within a reasonable time period (commensurate with the type of data stored on the media) and provide information on what information is on a missing device.
 - Protects information stored on removable media in accordance with the ODVs for the SC-28(1) Protection of Information at Rest | Cryptographic Protection control.
 - Returns NASA-owned removable media when no longer needed to fulfill NASA business needs, or upon termination of IT access. NASA data stored on non-NASA removable media should be dispositioned in accordance with applicable NASA policies (e.g., NPR 1441.1).

- Ensures that removable media are labeled in accordance with the MP-03 control. Removable media with a form factor that precludes legible marking (e.g., micro SD cards) should not be used to store information types which require marking (i.e., CUI).

3. Confidentiality and Sensitivity Definitions

FIPS 199 requires all federal information systems to be categorized based on the Confidentiality, Integrity, and Availability (CIA) security control requirements for such information systems, based on the potential impact of one of these security properties being compromised. These categorizations are also applied to media and information produced by or stored on information systems. From the perspective of media protection, the Confidentiality property is of greatest concern. Confidentiality is directly related to the concept of Sensitivity: the more sensitive the information on an information system or media item is, the higher its Confidentiality rating and requirements. CUI, and Personally Identifiable Information (PII) are examples of sensitive information.

FIPS 199 defines the loss of Confidentiality as “the unauthorized disclosure of information.” Thus, the release of information that is not sensitive and not covered by any designation that would render it confidential would be expected to have no adverse effect on organizational operations, organizational assets, or individuals and the information would not be considered confidential for the purposes of media protection.

All NASA information systems shall be designated as one of the following four *FIPS 199* Sensitivity/Confidentiality categories, as defined below:

- Sensitivity/Confidentiality is N/A: The National Aeronautics and Space Act of 1958 as amended⁶ Section 203(a)(3) instructs NASA to “provide the widest practicable and appropriate dissemination of information concerning its activities and the results thereof. All NASA information not otherwise protected by statute or regulation is therefore publicly available information and is non-sensitive, non-confidential information. For such information, the *FIPS 199* Confidentiality categorization is N/A.
- Low Sensitivity/Low Confidentiality: Unauthorized disclosure of this information would have a limited adverse impact on organizational operations, organizational assets, or individuals.
- Moderate Sensitive/Moderate Confidentiality: Unauthorized disclosure of this information would have a serious adverse impact on organizational operations, organizational assets, or individuals. See Section 5.3 for additional considerations.
- High Sensitivity/High Confidentiality: Unauthorized disclosure of this information could be expected to have severe or catastrophic adverse effect on organizational operations, assets, or individuals.

⁶ Public Law No. 85-568, 72 Stat. 426 (July 29, 1958).

The criteria for determining the Sensitivity and/or confidentiality of media are shown in Figure 1 below. Section 4 describes in detail the process for making this determination and the criteria used to do so.

Non-government owned computers shall be handled in accordance with the terms and conditions of the NASA contract that governs their use, if such contracts contain different requirements than are contained in this Handbook.

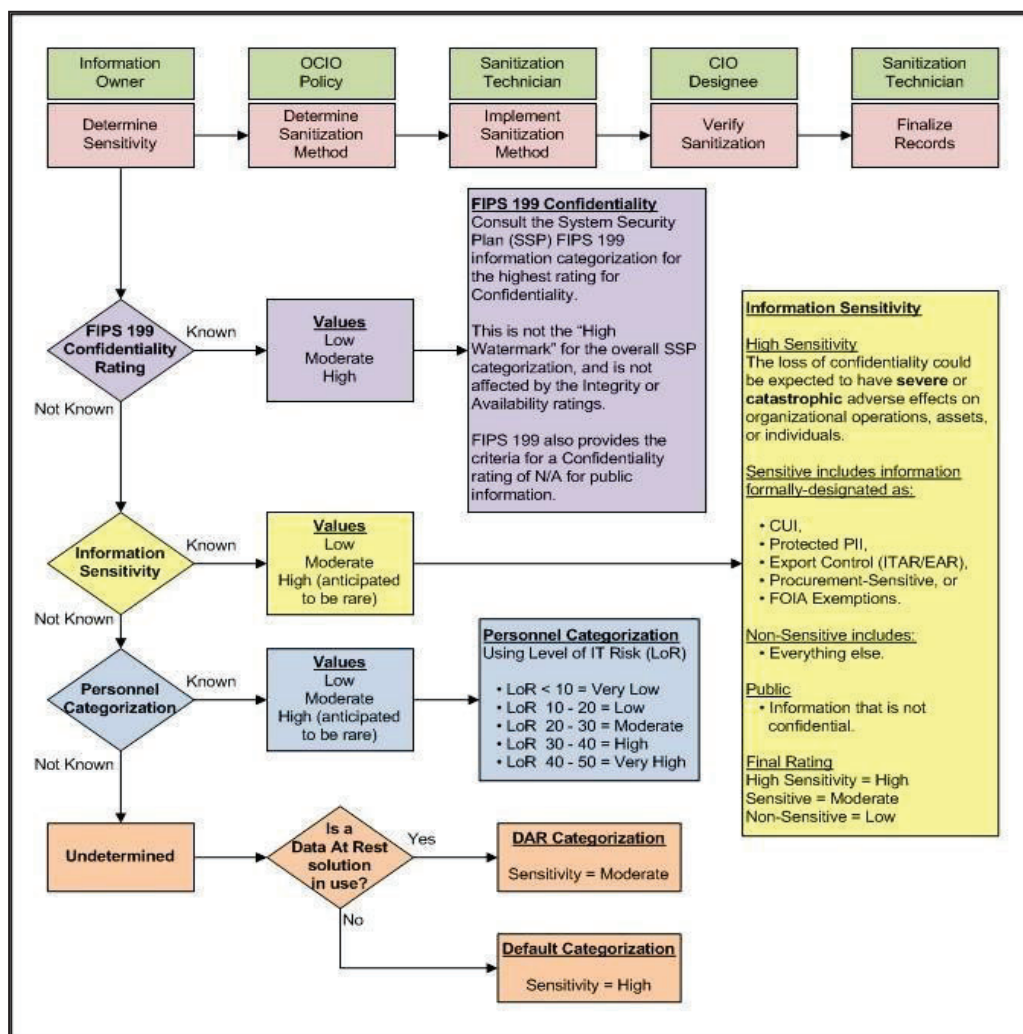


Figure 1: Media Confidentiality Sensitivity Determination Criteria

4. Determining Confidentiality and Sensitivity of Information

The ISO, in consultation with the IO, determines the Confidentiality designation for information on any digital media, or the device on which digital media resides (e.g., a laptop). Before determining the Confidentiality or Sensitivity of any media, the ISO and IO shall determine whether it is operable. If it is not, the media is subject to the Inoperable Media Sanitization process described in Section 8.2.

When a digital media device is first entered into service, or an existing device is being repurposed within NASA, or digital media (such as a hard drive) for a device is being replaced, it shall be assigned a rating at the highest level of Confidentiality and Sensitivity of the system to which it is assigned (Section 4.1) or the Level of IT Risk (LoR) of the User to which it is assigned (Section 4.2), whichever is higher.⁷

All media categorized as High for any reason (*FIPS 199* level of the associated system, user's LoR, or inability to make a determination and having no DAR solution present) or a special case shall be sanitized according to the Special Case Media Sanitization process, which is outlined in Section 8.4.

As noted in Section 9.5, Table 2, a media device may be repurposed at the same or higher level of Sensitivity or Confidentiality. If the device is assigned a High rating, it *may not* be repurposed at a lower level. However, there are some Low or Moderate level devices that, if properly sanitized, may be used at Low or N/A level (consult Section 8.5, Table 2 for more specifics).

The sequence of decisions for determining the Confidentiality and/or Sensitivity of media, and consequently how it is to be labeled and sanitized, is as follows:

- 1) Determine whether the media is operable (if not, sanitize it as described in Section 8.2).
- 2) Determine the Confidentiality of the system or systems to which it has access.
- 3) Determine the Sensitivity of the information on the media, based on the LoR of the user responsible for that media.
- 4) Categorize the media according to the Confidentiality of the system associated with the media or LoR of the user associated with the media, whichever is higher.
- 5) If neither the Confidentiality of the system associated with the media nor the LoR of the user associated with the media can be determined:
 - a) The media is presumed Moderate if it is protected with a DAR solution.
 - b) The media is presumed High if not protected with a DAR solution and/or determined to be "special case."
- 6) Ensure that the media is sanitized appropriately after use, using the Special Case Media Sanitization process (Section 8.4) if it is High or a special case, or the General Media Sanitization (Section 8.3) process if it is not.

Section 4.1 describes the process and criteria for categorizing media based on the *FIPS 199* rating of the system (or systems) to which it connects. Section 4.3 describes the process and criteria for determining a

⁷ Or whichever can be asserted with confidence. If neither the associated system rating nor responsible User's LoR can be asserted with confidence, then the media's Confidentiality/Sensitivity rating shall be presumed to be Moderate if the media is protected by a DAR solution. The types of information listed in Section 4.3 are typically categorized as being of Moderate sensitivity but may require additional considerations and/or prompt the ISO and IO to designate the media on which the information resides as a "special case." If the media is not protected by a DAR solution, or otherwise determined by the ISO and IO to be a special case, it is presumed to be High.

User's LoR and categorizing that User's media appropriately. Section 4.3 contains a list of types of special categories of information that are usually considered Moderate, but that may also require special consideration and prompt the ISO and IO to designate the media on which the information resides as a special case if it is not protected with a DAR solution.

Figure 2 below shows the workflow for determining the Confidentiality and Sensitivity of media.

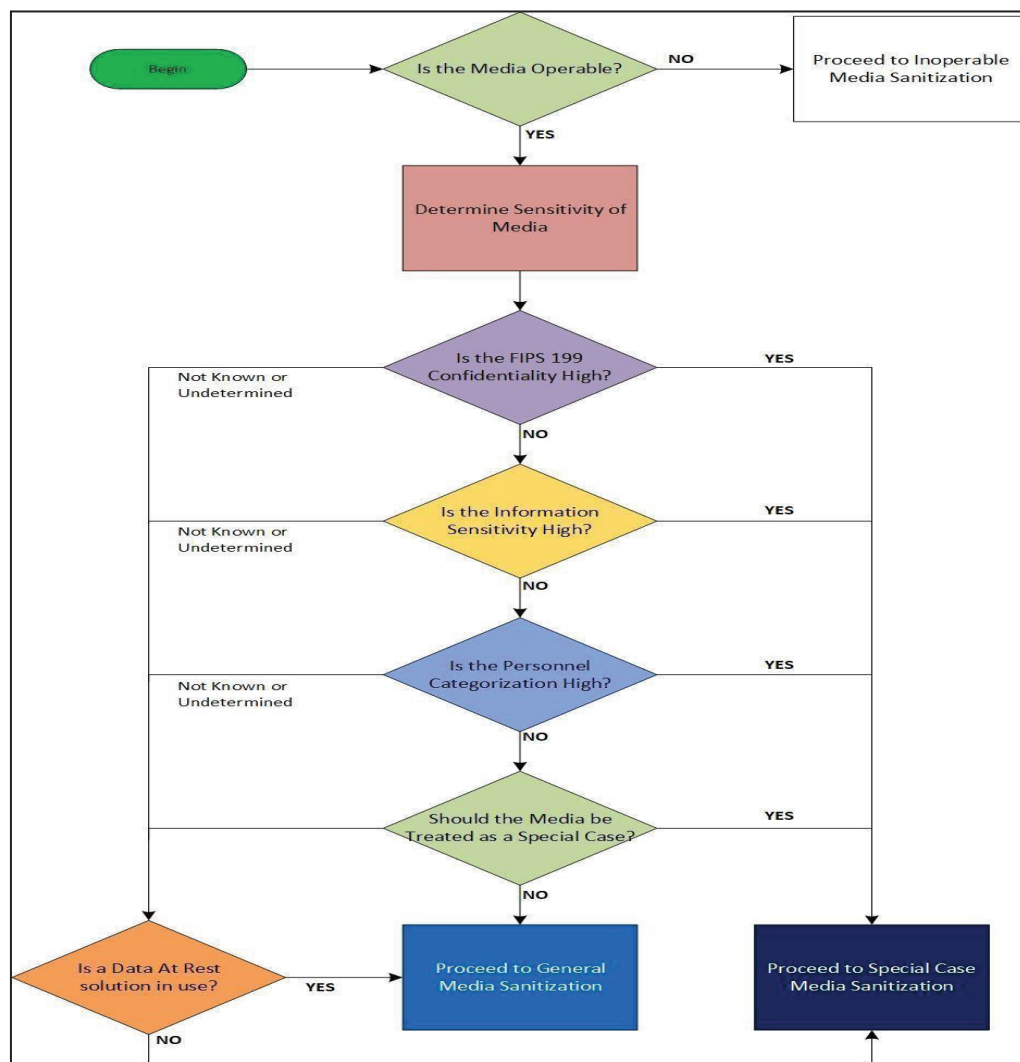


Figure 2: Media Confidentiality, Sensitivity, and Disposition Workflows

4.1 Establishing the Confidentiality Level of a System

The Confidentiality of a media item or device can be determined by reviewing the SSP of the system to which it connects. For example, a computer that accessed, accesses, or will access a Moderate Confidentiality system would be presumed to contain information of Moderate Confidentiality.

As required by *FIPS 199*, every SSP must assign a security level to the CIA security controls required within the system in order to assure its overall security.

- In establishing the overall security categorization of a system, NIST guidance uses the High Water Mark, which is the highest categorization of the three criteria of CIA. For example, many NASA systems have a High Water Mark of Moderate Impact based on a requirement for Availability and/or Integrity to be at that level, while the Confidentiality Impact may be Low or N/A.
- The Confidentiality categorization shall be the determining attribute for the level of confidential information on a system – the NIST High Water Mark may **not** be used.
- Under the NIST High Water Mark, many NASA systems are anticipated to have a Moderate Availability or Integrity categorization, while at the same time having a Low *FIPS 199* categorization for Confidentiality. In contrast, a *FIPS 199* categorization of High for the Confidentiality attribute is anticipated to be extremely rare for NASA systems.
- When multiple *FIPS 199* information Confidentiality levels are present on a device, the highest Confidentiality level shall be the Confidentiality designation for the device.

4.2 User-Based Sensitivity/Confidentiality Determination

When a User-based Sensitivity/Confidentiality determination is necessary, the Information System Owner, assisted if necessary by the Identity, Credential, and Access Management (ICAM) Center Business Process Lead (CBPL), will determine the User's categorization using the Identity Management and Account Exchange (IdMAX) system.

Every User (government and non-government) who has access to NASA information and systems has been assigned a logical LoR as defined in *NPR 2841.1*. This LoR Personnel Categorization can be used to establish the authorized level of information Sensitivity to which the User using the device could have had access.

- A numerical value of 10 or below represents a Very Low LoR to the Agency and thus no Sensitive NASA information may be presumed to be resident on any such User's digital media.
- A numerical value of between 10 and 20 below represents a Low LoR and thus only Non-Sensitive NASA information, such as their own privacy data, may be presumed to be resident on any such User's digital media.
- A numerical value between of 20 to 30 represents a Moderate LoR and thus information only up to the level of Moderate Sensitivity, such as other people's privacy data, CUI data may be presumed to be on the User's digital media.
- A numerical value between 30 and 40 or above represents a High LoR and thus information up to the level of High Sensitivity, such as access to command and control systems, human flight, and human safety systems may be presumed to be on the User's digital media.

- A numerical value of 41 or above represents a Very High LoR. Media with this LoR is beyond the scope of this document. Further instruction for proper disposition shall be immediately sought from the Office of Protective Services.

4.3 Special Considerations

For purposes of determining the appropriate sanitization level, the Moderate categorization may include information categorized as Moderate based on any number of considerations. For Moderate Confidentiality information formally designated or labeled⁸ as one or more of the following sensitive information categories, additional considerations may be applied.

Information categorized at the Moderate level may include information that originated within NASA or was provided to NASA by another Federal Department or Agency and includes the following types of information:

- Controlled Unclassified Information (CUI);
- PII as defined by *NPR 1382.1* and associated statutes;
- Restricted procurement information as defined in 41 USC § 423 and the Federal Acquisition Regulations (FAR) section 3.104; and
- Other information required by law or Federal regulation to be protected from disclosure, where that disclosure results in more than a limited adverse impact (i.e., higher rating than Low Sensitivity).

If Moderate information falls into the categories of information set out in the list above and is NOT protected by a NASA DAR encryption solution, for the purposes of sanitization, or other disposition of the media, the ISO in consultation with the IO may treat the media as if it is at a High Sensitivity/Confidentiality level and shall follow the requirements as set out in Section 8.5, Table 2.

5. Tagging Media Based on Confidentiality and Sensitivity Ratings

As part of a life-cycle process covering device acquisition through disposal or disposition, as new devices are acquired that contain media capable of storing, processing, or transmitting NASA information, the

- For all newly procured devices,

⁸ For guidance IOs and ISOs may use, and should rely on, the system data type categorizations already documented on the system's NF1748 and in their SSPs. tagging procedures set out in this Section shall apply, to include all authorized external media such as USB removable media.

As described in Section 4, digital media devices shall be assigned a Confidentiality and Sensitivity rating across their lifecycle:

- For any device at the time it is repurposed within NASA, or
- For any device when the digital media (such as a hard drive) is replaced.⁹

For digital media that do not fall within the provisions listed at the beginning of Section 4, implementation of the life-cycle tracking system described herein shall be optional. However, the sanitization and the inspection and verification requirements of this Handbook shall still be applied, as set out in Section 9 and Section 10.

At the time of the issuance of a new device, or the repurposing within NASA of an existing device, a permanent record of the Confidentiality and Sensitivity rating for the device shall be entered into the facility or contractor permanent property or asset management record for the device.

For ease of identification, at the time of issuance, a device shall also be marked with an indelible Media Confidentiality and Sensitivity Tag (to be provided by the CO and/or COTR based upon input from the ISO). The tag shall be on the underside of the external case of the device, and shall remain there until the sanitization process is complete and verified. (If a device is being repurposed to a higher level, the original tag may be supplemented by a second, higher-level tag and the appropriate change to the property record, or asset management record, may also be made.)

The tag types shall be as follows:

- A white tag shall indicate that the device may never contain higher than publicly available information.
- A green tag shall indicate that the device may never contain higher than Low Confidentiality and Sensitivity information.
- A yellow tag shall indicate that the device may never contain higher than Moderate Confidentiality and Sensitivity information.
- A red tag shall indicate that the device may contain High Confidentiality and Sensitivity information. (Note that per Section 1.2, this Handbook does not apply to Classified National Security Information.)

If digital media are removed from the external casing containing the indelible tag identified in the preceding list, the digital media itself must be marked with an identical tag and handled, sanitized, inspected and verified, and dispositioned as set out in Sections 7, 8, and 9.

Due to the complexity of sanitizing certain devices to assure they can be reused and will not have to be destroyed as part of the sanitization process, some devices shall not be authorized to contain categories of NASA information, such as devices that utilize solid-state memory as identified in Section 8.5, Table 2.

⁹ Although NASA and NASA Contractor personnel must begin tracking the device's lifecycle from acquisition on, the requirement for life cycle tracking of digital media does not apply retroactively.

6. Digital Media Sanitization Considerations

Digital Media Sanitization is the process of removing electronic data from storage devices with a degree of certainty that corresponds to the risk levels incorporated in the *FIPS 199* Confidentiality categorization. The higher the Confidentiality categorization, the more assurance is necessary that information is sanitized commensurate with the potential harm that could result from its unauthorized disclosure. Thus High Sensitivity, High Confidentiality information must be impossible, or nearly impossible, to recover.

The sanitization method used shall vary with different types of digital storage media and devices.¹⁰

Sanitization of IT devices leaving the control of NASA shall include the physical removal of any external labels or markings that provide information about internal technical details regarding NASA networks, information, or information systems. Examples include:

- NASA organizational identification, status labels, or markings;
- Device location or activity log information; or
- Device or network names, addresses or routing information.
- Permitted removal of such external labels DOES NOT include the Media Confidentiality and Sensitivity Tag referenced in the list at the end of Section 5.

For digital media devices leaving NASA control, the User shall only remove labels or markings of the type described in the list above. Removal shall be confirmed at the time of disposal by the PDO. However, the Media Confidentiality and Sensitivity Tag shall be left on the device by the User.

The Confidentiality and Sensitivity Tag shall only be removed by the PDO if the digital media device is leaving the control of NASA, and only after sanitization has been completed, inspected, and verified.

According to *NIST SP 800-88*, there are multiple methods for sanitizing storage devices, which are defined below in the context of the information Confidentiality or Sensitivity Categorization:

- Media Disposal (Sensitivity or Confidentiality Categorization is N/A): Disposal is the act of discarding media with no unaddressed sanitization considerations. However, for NASA, even digital storage media that are thought to contain only publicly available, non-sensitive information shall undergo a form of sanitization, as specified in Section 8.5, Table 2.

¹⁰ For example, computer hard drives require different sanitization procedures than do smart phones or external flash memory devices.

- Media Clearing (Sensitivity or Confidentiality Categorization is Low): A level of media sanitization intended to protect the Confidentiality of information against a robust keyboard attack. Clearing shall not allow information to be retrieved by data, disk, or file recovery utilities.¹¹
- Media Purging (Sensitivity or Confidentiality Categorization is Moderate): A media sanitization process that protects the Confidentiality of information against a laboratory-style attack using signal processing equipment and specially trained personnel.¹²
- Media Destruction (Sensitivity or Confidentiality Categorization is High): The ultimate form of sanitization resulting in media that cannot be reused due to shredding, disintegration, incineration, pulverization, melting, crushing, degaussing, or a combination thereof. Destruction shall be the ONLY means by which optical media (created and read using laser devices) are sanitized.
 - Due to the hazardous materials that may be present in digital media, all safety and any special disposal requirements shall be identified and addressed prior to media destruction.

7. Digital Media Sanitization Specifics

Any digital storage device that has ever contained non-public NASA information, even for a brief period of time, shall be appropriately sanitized before it can be transferred for:

- Maintenance,
- Replacement or repair,¹³
- Reuse/repurposing,
- Disposal or recycling,
- Gifting to schools per the Stevenson-Wydler Technology Innovation Act of 1980 and the Computers for Learning Program as authorized by Executive Order 12999, or
- Pursuant to the terms and conditions of a NASA contract.

The nature of the digital media may require different actions to achieve the sanitization objective for the required Confidentiality or Sensitivity level as set out in Section 8.5, Table 2.

¹¹ For example, overwriting is an acceptable method for clearing media. Studies have shown that most of today's media can be effectively cleared by one overwrite per *NIST SP 800-88, Supra*, Table 2-1, pg. 7.

¹² For Advanced Technology Attachment (ATA) disk drives manufactured after 2001 (over 15 GB), the terms "Clearing" and "Purging" have converged. Executing the firmware Secure Erase command (for ATA-based drives only) and degaussing are examples of acceptable methods for purging. (Degaussing is exposing the magnetic media to a strong magnetic field used to sanitize magnetic media.) However, unlike use of the Secure Erase command, proper degaussing of any hard drive assembly usually renders the drive unusable since the firmware that manages the device is also irreparably purged.

¹³ An exception for warranty replacement or warranty repair is contained in Section 12.

7.1 Approved Sanitization Tools

The NASA Office of the CIO (OCIO) maintains a specific list of approved tools for digitally sanitizing and/or physically destroying media. Tools that have not been approved for use by the NASA OCIO shall be deemed as not acceptable for sanitization of digital media or destruction of physical media containing NASA information.

If any NASA organization or contractor believes that a tool other than the ones listed in this section would improve effectiveness or efficiency, the cognizant Center CIO must propose the tool to the NASA OCIO for consideration.

7.1.1 Digital Media Sanitization Tools

For the digital sanitization of certain digital media storage devices, the NASA OCIO has approved the use of the tools listed in Table 1 below. This section applies to places where we have hard drives or other physical media. We will have different procedures for cloud-based services, which can be arranged upon requesting such services.

Table 1: Approved Media Sanitization Tools¹⁴

Product Name	Website
SecureErase	https://cmrr.ucsd.edu/resources/secure-erase.html
WipeDrive/WipeDrive Pro	https://www.whitecanyon.com

7.1.2 Physical Media Destruction Tools

For smart card devices & data storage tokens that are in credit card form, cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder (nominal 2 mm wide cuts). Smart cards packaged into tokens (i.e., SIM chips, thumb drives and other physically robust plastic packages) that are not capable of being shredded must instead be destroyed via incineration or disintegration into particles 2 mm in size.

The National Security Agency (NSA) provides a list of evaluated products that are acceptable and approved for high-security disintegrators, optical storage destruction devices, punched tape destruction devices, and degaussers. Within the context of Section 8.5, Table 2, devices on the NSA list may be used by NASA and NASA contractor personnel to destroy media. This list can be found at the following website: <https://www.nsa.gov/resources/everyone/media-destruction/>

¹⁴ Configuration settings for the Agency Approved Media Sanitization Tools are found in Appendix D.

Refer to *NPR 1600.2* for further specifications on approved physical destruction methods for media including magnetic storage devices. Table 2 in Section 9.5 provides guidance on methods of physical destruction for various types of media based on sensitivity level.

7.2 Recording and Verifying Sanitization

In order to ensure proper record keeping and fully meet NASA requirements, the Media Sanitization Record form in Appendix D shall be used to record and track the sanitization of High or Moderate security impact storage media. Use of the Media Sanitization Record form shall be optional for systems with a security impact level of Low or Not Applicable (N/A).¹⁵

In addition to sanitization and record keeping activities, it is also necessary to routinely test the sanitization equipment, processes, procedures, and personnel to ensure they are performing as intended (as noted in Sections 7 and 8).

7.3 Records Retention Compliance

- Prior to initiating sanitization, all Users shall be required to ensure appropriate handling of Federal Records per *NPR 1441.1*.
- Questions regarding records retention shall be directed to the Center Records Manager for assistance prior to submitting digital media devices for sanitization.

Specific sanitization requirements are set out by digital media type in Section 8.5, Table 2 based on the Confidentiality or Sensitivity level.

When there is doubt about the Sensitivity/Confidentiality level of a device, refer specifically to Section 5 of this document.

8. Sanitization Instructions for Media Types

Sanitization procedures shall vary by media type. The level of rigor for sanitization procedures increases as the level of Sensitivity or Confidentiality increases. This is because the potential harm that might result from the unauthorized disclosure of NASA information increases with the level of Sensitivity or Confidentiality.

Table 2 in Section 8.5 below sets out the criteria that shall be followed under this instruction.

- Devices cited in Table 2 are authorized to be repurposed within NASA to an authorized IdMAX user at the same or higher level of Confidentiality or Sensitivity.

¹⁵ The requirement to use the Media Sanitization Record form in Appendix C may be substituted for an electronic alternative, if *all* of the information on the Media Sanitization Record is tracked (and retrievable) by another electronic method, such as an inventory database.

- Repurposing pursuant to Item 1 on this list is NOT authorized for use at a lower level of Sensitivity/Confidentiality.

Devices that contain High Sensitivity/Confidentiality information may be repurposed within NASA to an authorized IdMAX user at the High level ONLY after following the sanitization process in Table 2 at the Moderate level. For instances where High and Moderate have the same sanitization requirement, following the sanitization process in Table 2, the lower of the two levels is authorized for use.

- The lower standard of sanitization set out above is authorized because of the following compensating IT security controls:
 - The new NASA User has complied with NASA personnel security policy and procedures, and
 - The new NASA User has completed the required annual NASA security awareness and training policy and procedures.
- Verification need not be performed for repurposed devices that comply with Item 1 on this list.
 - All High Confidentiality media that are not being repurposed within NASA, as set out in this list, shall be destroyed

For devices containing digital media that can be readily removed (for example, a hard drive), the sanitization process shall be performed only on the digital media rather than the entire device. However, for devices that do not have readily removable media, the sanitization process shall be conducted on the entire unit.

In some instances, a two-step process shall be required. For example, a smart phone with a SIM card shall be treated as two sanitization processes: one for the SIM card, and one for the phone's internal memory.

To foster reutilization of digital devices and to minimize the generation of potentially hazardous waste, when sanitizing digital storage media, the least destructive method may be used commensurate with potential risk and with this Handbook, except as noted below.

- For the closeout of large projects, such as the retirement of the Space Shuttle fleet or the end of life of a large number of computer tapes, the most cost-effective end of life process for digital media may require a different approach.
- For the closeout of such large legacy projects, with the approval of the local CIO, CISO, and the PDO, all digital media may be treated as High Sensitivity/Confidentiality and may be destroyed utilizing the mechanisms set out in Section 8.5, Table 2.

8.1 Media Documentation and Sorting

Certain procedures for media classification and handling may differ depending upon the condition of media (e.g., whether it is inoperable or not), but in all cases the ISO or MSP¹⁶ is responsible for properly documenting and organizing media prior to passing it on for sanitization or destruction.

The ISO/MSP shall completely and thoroughly document the inventory information from the digital media device and collect, at minimum, the following information:

- Manufacturer
- Model information
- Serial Number
- Device Type
- Media Confidentiality and Sensitivity Tag information
- Any NASA organizational identification
- Device location information
- Device name (if applicable)

After completely and thoroughly documenting the inventory, the ISO shall gather and sort like media devices into batches such that all items in the batch are similar to each other in terms of their type, confidentiality and sensitivity categorization, and the sanitization requirements as listed in Table 2.

The ISO/MSP shall then ensure that the batched and inventoried media is secured in a manner that is not easily accessible to unauthorized personnel, and if required, in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable law, regulations, and government-wide policies for protecting and securing government data.

The batched, inventoried, and secured devices shall then be permitted to proceed to the Media Sanitization or Media Destruction process, depending upon the state of the media (operable or inoperable).

8.2 Inoperable Media Sanitization¹⁷

When a digital media device is deemed to be inoperable, or when the sanitization processes defined in Table 2 cannot be implemented, the device shall be destroyed by following the Inoperable Media Sanitization Workflow process:

¹⁶ In most cases the ISO will be responsible for carrying out the actions described in this section. The MSP is responsible under certain conditions for Special Case Media Sanitization as described in Section 9.4

¹⁷ An exception from the requirement to destroy inoperable devices that are leaving NASA's control for warranty replacement or warranty repair can be found in Chapter 11.

- 1) Document the inventory of media.
- 2) Batch like media items together.
- 3) Secure the media as appropriate to its Sensitivity rating.
- 4) Proceed to the Media Destruction process described in Section 10.

The process is also outlined in Figure 3 below.

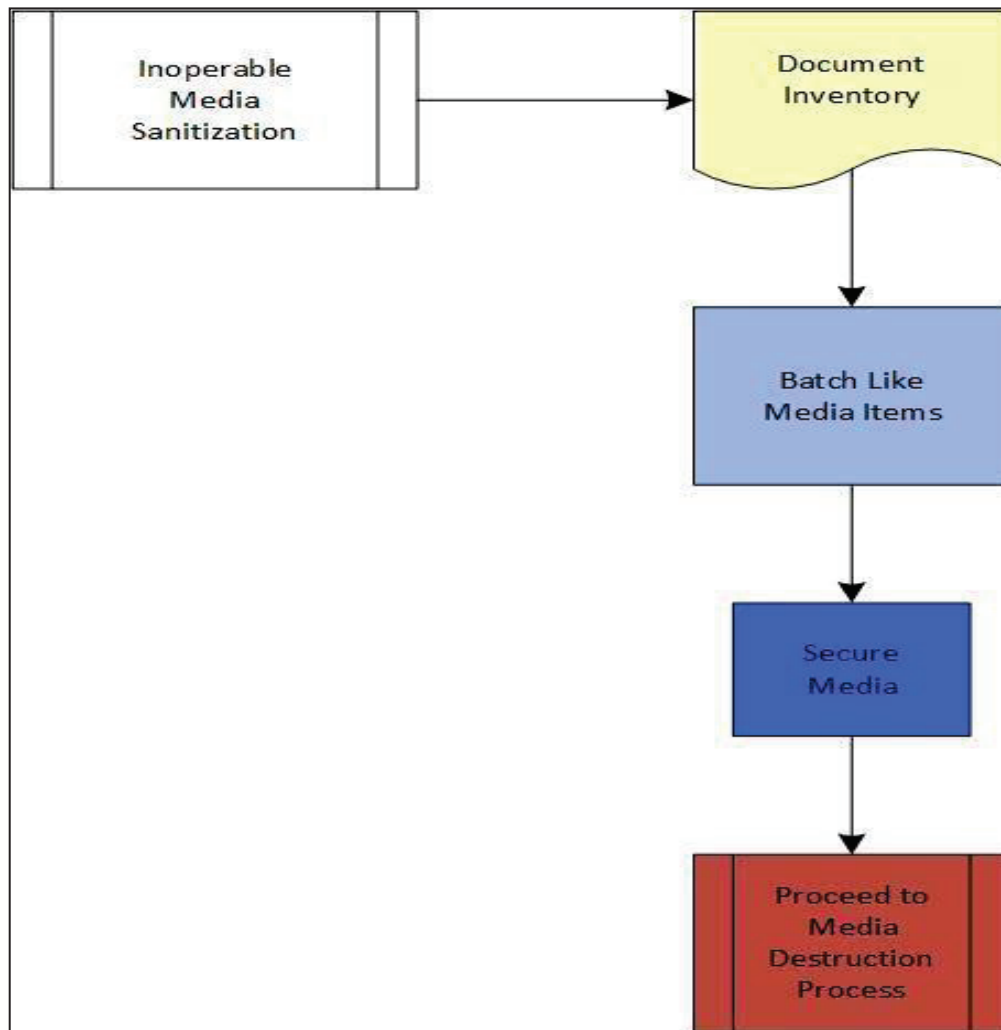


Figure 3: Inoperable Media Sanitization Workflow

If the Sensitivity Determination Workflow as described in Section 4, Figure 2, yields a determination that a digital media device is inoperable, the ISO shall follow the steps described in Section 8.2 before proceeding to the Media Destruction Process described in Section 10.

8.3 General Media Sanitization

If the Sensitivity Determination Workflow as described in Section 4, Figure 2 yields a determination that a digital media device shall be sanitized according to the General Media Sanitization process, the MSP and the ISO shall perform portions of the following actions to complete the General Media Sanitization Workflow.

The ISO determines if the media:

- 1) Can be re-used.
 - a) If the determination is No, the ISO shall proceed to “Will Media Leave NASA’s Control?”
 - b) If the determination is Yes, the ISO shall proceed to “At the Same Sensitivity Level?”
- 2) Can be re-used at the same sensitivity level.
 - a) If the determination is No, the ISO shall proceed to “At a Lower Sensitivity Level?”
 - b) If the determination is Yes, the ISO shall proceed to “Sanitize Media According to NASA Policy.”
- 3) Can be re-used at the lower sensitivity level.
 - a) If the determination is Yes, the ISO shall proceed to “Sanitize Media According to NASA Policy.”¹⁸
 - b) If the determination is No, the ISO shall proceed to “Will Media Leave NASA’s Control?”
- 4) Will be leaving NASA’s control¹⁹
 - c) If the determination is Yes, the ISO shall proceed to “Document Inventory.”
 - d) If the determination is No, the ISO shall proceed to “Sanitize Media According to NASA Policy.”

This decision process is outlined in Figure 4 below.

¹⁸ This may only occur where Section 8.5, Table 2 permits such re-use.

¹⁹ An exception from the requirement to destroy devices that are leaving NASA’s control solely for warranty replacement or warranty repair can be found in Section 11.

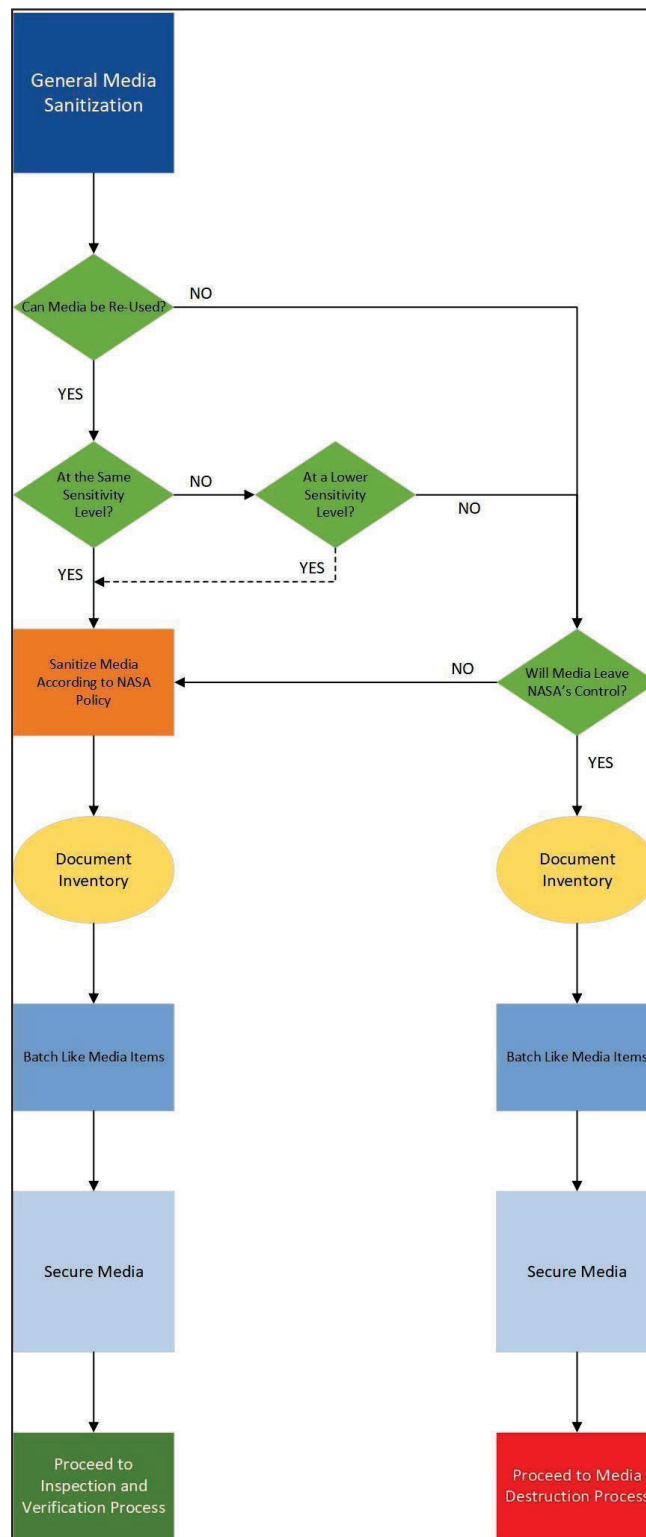


Figure 4: General Media Sanitization Workflow

The ISO follows the steps described in Section 8.1 before the media can proceed to the Inspection and Verification Process outlined in Section 9.1.

8.4 Special Case Media Sanitization

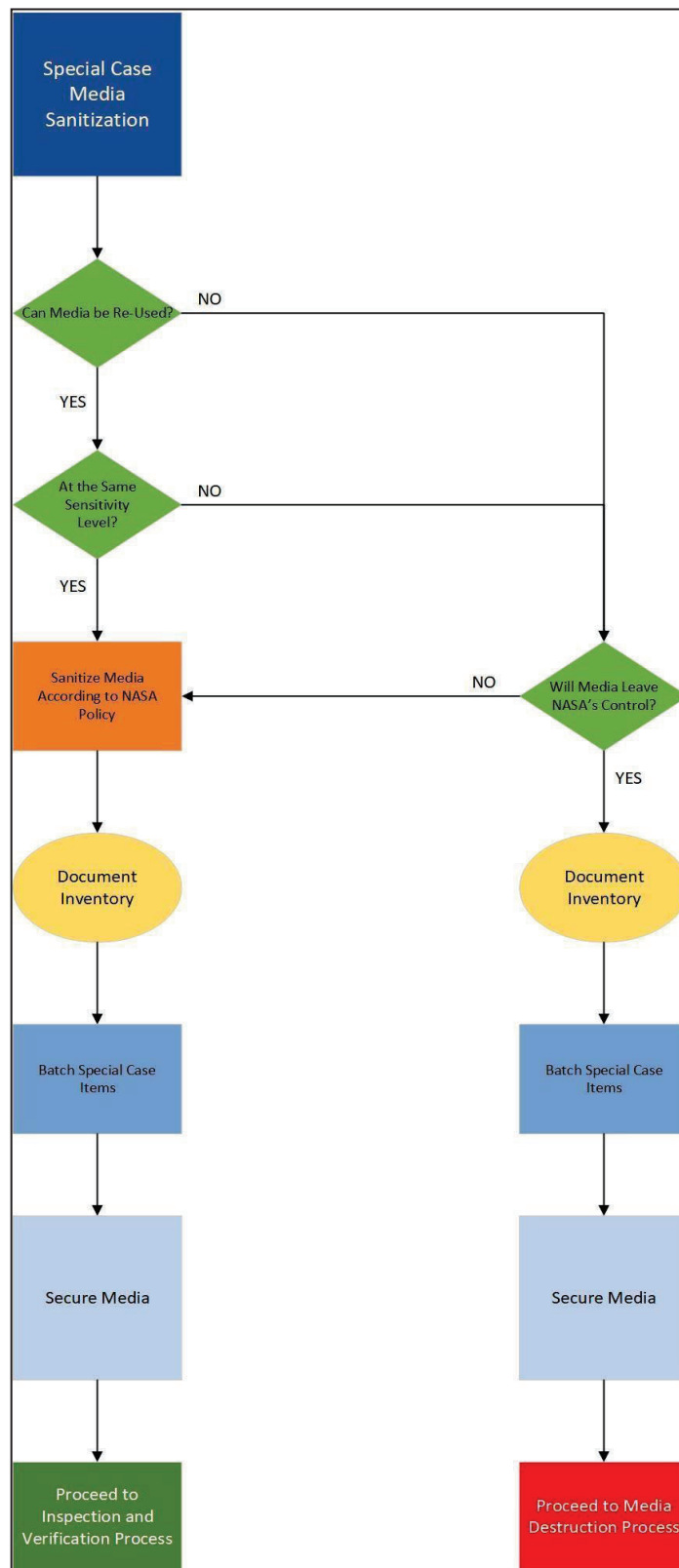
If the Sensitivity Determination Workflow yields a determination that a digital media device shall be sanitized according to the Special Case Media Sanitization process, MSP and the ISO complete the Special Case Media Sanitization Workflow, as outlined in Figure 5 below.

The workflow shall begin with the ISO determining whether the media:

- 1) Can be re-used.
 - a) If the determination is No, the ISO proceeds to “Will Media Leave NASA’s Control?”
 - b) If the determination is Yes, the ISO proceeds to “At the Same Sensitivity Level?”
- 2) Can be re-used at the same sensitivity level.
 - a) If the determination is No, the ISO proceeds to “Will Media Leave NASA’s Control?”
 - b) If the determination is Yes, the ISO proceeds to “Sanitize Media According to NASA Policy.”
- 3) Will be leaving NASA’s control²⁰
 - a) If the determination is Yes, the ISO proceeds to “Document Inventory.”
 - b) If the determination is No, the ISO proceeds to “Sanitize Media According to NASA Policy.”

Note that if the media is leaving NASA’s control (and therefore bound for destruction), the ISO shall perform the series of actions described in Section 9.1. Otherwise, the MSP takes responsibility for the media.

²⁰ An exception from the requirement to destroy inoperable devices that are leaving NASA’s control for warranty replacement or warranty repair can be found in Section 11.

*Figure 5: Special Case Media Sanitization Workflow*

If the media is leaving NASA's control, the ISO is responsible for performing the actions listed in Section 8.1 before the media can be submitted for the Media Destruction Process outlined in Section 10. Otherwise, the MSP is responsible for performing those steps prior to the Media Sanitization Process.

8.5 Media Sanitization Requirements Based on Confidentiality and Sensitivity

Table 2 below specifies sanitization procedures for different types of media depending on the device and its Confidentiality/Sensitivity rating.

The NASA CIO welcomes feedback regarding the effectiveness and efficiency of the methods described in Table 2 and/or any recommendations for enhancement.

If any NASA organization, or contractor, believes another method would improve effectiveness or efficiency, the Center CIO must propose the method to the NASA OCIO for consideration. A method which has not been approved for use by the NASA OCIO is deemed ***not acceptable*** for sanitization of digital media containing NASA information.

Table 2: Media Sanitization Requirements based on Confidentiality or Sensitivity²¹

	Confidentiality or Sensitivity Level			
Media Type	N/A	Low	Moderate	High
Hand-Held Devices				
Cell Phones and Personal Digital Assistants (PDAs) that ARE NOT capable of NASA email or general Internet browsing	Manually delete all information, such as calls made and phone numbers stored, then perform a full manufacturer's reset to reset the cell phone back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.	Use of this device is not approved for this level of Confidentiality or Sensitivity. If Moderate or High Confidentiality or Sensitivity information is inadvertently installed on such a device, then at end of life, the device must be shredded, disintegrated, pulverized, or incinerated in a licensed incinerator. However, the device may be repurposed within NASA to an authorized IdMAX user at the same level (but not a lower level) of Confidentiality or Sensitivity by following the instructions for Low Sensitivity.		

²⁰ If destruction is the most cost-effective process to sanitize a certain type of digital media, then destruction may be favored over another type of media sanitization. However, the process for destruction shall conform to the requirements of this Handbook (i.e. shredding, disintegration, pulverization, or incineration).

²¹ If destruction is the most cost-effective process to sanitize a certain type of digital media, then destruction may be favored over another type of media sanitization. However, the process for destruction shall conform to the requirements of this Handbook (i.e., shredding, disintegration, pulverization, or incineration).

	Confidentiality or Sensitivity Level			
Media Type	N/A	Low	Moderate	High
Cell and Smart Phones, PDAs, and tablet or tablet-like devices that ARE capable of NASA email or general Internet browsing	Manually delete all information, such as calls made and phone numbers stored, then perform a full manufacturer’s reset to reset the cell phone back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure. If at the end of life, or if the device is targeted to be sent outside NASA, and Moderate Confidentiality or Sensitivity information is present on the device, then device shall not be permitted to sold, donated, or otherwise dispositioned. The device shall be shredded, disintegrated, pulverized, or incinerated.			These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same Confidentiality or Sensitivity level by following the instructions for Moderate Sensitivity. If at end of life, shred, disintegrate, pulverize, or incinerate.
Networking Devices				
Networking Devices (all types)	Perform a full manufacturer’s reset to reset the networking device back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure			These devices may be repurposed within NASA ONLY to an authorized system at the same Confidentiality or Sensitivity level, and may follow the instructions for Moderate Sensitivity. If at end of life, shred, disintegrate, pulverize, or incinerate.
Office Equipment				
	Confidentiality or Sensitivity Level			
Media Type	N/A	Low	Moderate	High

Copy Machines	<p>Perform a full manufacturer's reset to reset the copy machine to its factory default settings.</p> <p>** Please contact the manufacturer for proper sanitization procedure.</p>	<p>These devices may be repurposed within NASA ONLY to an authorized system at the same Confidentiality or Sensitivity level, and may follow the instructions for Moderate Sensitivity. If at end of life, remove digital storage media to shred, disintegrate, pulverize, or incinerate.</p>
Fax Machines	<p>Perform a full manufacturer's reset to reset the fax machine to its factory default settings.</p> <p>** Please contact the manufacturer for proper sanitization procedures. Some older fax machine use a physical medium similar to carbon paper that retains a copy of an incoming fax which shall be removed and shredded or incinerated.</p>	<p>These devices may be repurposed within NASA ONLY to an authorized system at the same Confidentiality or Sensitivity level, and may follow the instructions for Moderate Sensitivity. If at end of life, remove digital storage media to shred, disintegrate, pulverize, or incinerate.</p>

	Confidentiality or Sensitivity Level			
Media Type	N/A	Low	Moderate	High
Printers	Perform a full manufacturer’s reset to reset the fax machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedures.			These devices may be repurposed within NASA ONLY to an authorized system at the same Confidentiality or Sensitivity level, and may follow the instructions for Moderate Sensitivity. If at end of life, remove digital storage media to shred, disintegrate, pulverize, or incinerate.
Generic Disk Drives				
ATA and SATA Hard Drives (not including solid-state versions)	If the media is being repurposed within NASA, the media shall be either reimaged with a NASA standard image, or sanitized the using the Secure Erase command. If the media is being sent outside NASA, sanitize media by using agency-approved tools.	If the media is being repurposed within NASA, the media shall be sanitized using the Secure Erase command, and a second agency approved software tool shall be used to do a one pass overwrite. If the media is being repurposed within NASA, the media may be reimaged with a NASA standard image. If the media is being sent outside NASA, sanitize media by using agency-approved tools.	These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same Confidentiality or Sensitivity level by following the instructions for Moderate Sensitivity. If at end of life, degauss and crush; or shred, disintegrate, pulverize, or incinerate.	

	Confidentiality or Sensitivity Level			
Media Type	N/A	Low	Moderate	High
SCSI, SAS, and Fibre Channel Drives	Sanitize media by using agency-approved tools.		Sanitize media by using agency-approved tools.	These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same Confidentiality or Sensitivity level by following the instructions for Moderate Sensitivity. If at end of life, degauss and crush; or shred, disintegrate, pulverize, or incinerate.
Solid State Drives, including USB-based Removable Media: (a.k.a. Pen Drives, Thumb Drives, and Flash Drives). Includes HSDL and PCI-E direct-attached variants.	Sanitize media by using agency-approved tools that implement a secure erase command directly on the media device.		These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same or higher Confidentiality or Sensitivity level by following the instructions for Low Sensitivity. If at end of life and crushing. Alternatively sanitize by shredding, disintegrating, pulverizing, or incinerating.	
Magnetic Disks				
	Confidentiality or Sensitivity Level			
Media Type	N/A	Low	Moderate	High
Floppies	Sanitize media by using agency-approved tools.		These devices may be repurposed within NASA ONLY at the same or higher Confidentiality or Sensitivity level by following the instructions for Low	These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same Confidentiality or Sensitivity level by following the instructions for Low

		Sensitivity. If at end of life, degauss in an NSA/CSS-approved degausser.	Sensitivity. If at end of life, degauss and crush; or shred, disintegrate, pulverize, or incinerate in a licensed facility.
Zip Disks	Sanitize media by using agency-approved tools.	These devices may be repurposed within NASA ONLY at the same or higher Confidentiality or Sensitivity level by following the instructions for Low Sensitivity. If at end of life, degauss or sanitize using the Secure Erase command. Use a second NASA approved software tool (DBAN or WipeDrive) to do a one pass overwrite.	These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same Confidentiality or Sensitivity level by following the instructions for Low Sensitivity. If at end of life, degauss and crush; or shred, disintegrate, pulverize, or incinerate in a licensed facility.

	Confidentiality or Sensitivity Level			
Media Type	N/A	Low	Moderate	High
Magnetic Tapes				
Reel and Cassette Format Magnetic Tapes	These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same or higher Confidentiality or Sensitivity level. If at end of life, clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods.	These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same or higher Confidentiality or Sensitivity level by following the instructions for Low Sensitivity. If at end of life, degauss using an NSA/CSS-approved degausser.	These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same Confidentiality or Sensitivity level by following the instructions for Low Sensitivity. If at end of life, Incinerate by burning the tapes in a licensed incinerator or shred. Preparatory steps, such as removing the tape from the reel or cassette prior to destruction, are unnecessary as part of NASA policy; However, segregation of components (tape and reels or cassettes) may be necessary to comply with the requirements of a destruction facility or for recycling measures.	
	Clearing by Overwriting shall be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified or sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape shall be overwritten one time with known non-sensitive signals. At end of life, destruction as if High Sensitivity may be most efficient option.	Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. At end of life, destruction as if High Sensitivity may be most efficient option.		

	Confidentiality or Sensitivity Level			
Media Type	N/A	Low	Moderate	High
Optical Disks				
CDs/DVDs/Blue Ray	Shred	Shred	Shred, disintegrate, pulverize, or incinerate in a licensed facility.	
Internal Memory				
Compact Flash Cards/Drives, SD, Sony MemoryStick™	Sanitize media by using agency-approved tools.		These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same or higher Confidentiality or Sensitivity level by following the instructions for Low Sensitivity. If at end of life, shred, disintegrate, pulverize, or incinerate in a licensed facility.	
Magnetic Core Memory	If practicable, sanitize media by using agency-approved tools. Otherwise see instructions for High.		These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same or higher Confidentiality or Sensitivity level by following the instructions for Low Sensitivity. If at end of life, shred, disintegrate, pulverize, or incinerate in a licensed facility. When practical, the outer chassis and electronic circuit boards shall be removed from the core memory unit to optimize destruction.	
PC Cards or Personal Computer Memory Card International Association (PCMCIA) Cards	These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same or higher Confidentiality or Sensitivity level. If at end of life, shred, disintegrate, pulverize, or incinerate by burning in a licensed incinerator. If disintegrating, use an NSA-evaluated disintegrator to reduce the card's internal circuit board and components to particles that are nominally two (2) millimeters in size.			
Smart Cards	For smart card devices & data storage tokens that are in credit card form, cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder (nominal 2 mm wide cuts). Smart cards packaged into tokens (i.e. SIM chips, thumb drives and other physically robust plastic packages) that are not capable of being shredded must instead be destroyed via incineration or disintegration to 2 mm size particles. These devices must not be repurposed.			

	Confidentiality or Sensitivity Level			
Media Type	N/A	Low	Moderate	High
Magnetic Cards				
Magnetic Cards	Sanitize media by using agency-approved tools.		These devices may be repurposed to an authorized IdMAX user within NASA ONLY at the same or higher Confidentiality or Sensitivity level by following the instructions for Low Sensitivity. If at end of life, shred, disintegrate, pulverize, or incinerate.	
Other				
Media types not covered above	These devices may be repurposed to an authorized IdMAX user, or to an authorized system, within NASA ONLY at the same or higher Confidentiality or Sensitivity level. Use methods from other media types and Confidentiality or Sensitivity Level to the extent that sanitization can be verified. If the sanitization cannot be verified, then destroy the media (shred, pulverize, or incinerate in a licensed facility).			

9. Digital Media Inspection and Verification (Sampling)

Sampling, or inspection and verification, provides one means of verification that a population of media asserted to be sanitized conforms with the requirements of a technical specification – in the context of this Handbook, a pass/fail characteristic. The process of inspecting and verifying that digital media sanitization has been correctly and effectively performed requires:

- Utilization of a sampling methodology,
- Establishment of inspection criteria, and
- Establishment of a rejection limit to determine if a batch should be accepted or rejected.

The establishment of inspection criteria is generally a pass/fail test that is performed on digital media. However, the inspection criteria are specific to each type of digital media and sanitization method used on that media. For example, a computer hard drive that has been sanitized by degaussing has different inspection criteria than the same hard drive that was sanitized by re-imaging. The process of inspection and verification, if conducted properly, shall allow the MIVP and by extension the CIO, to assert to a level of 90% confidence, a conclusion about the characteristic of a population.

9.1 Digital Media Inspection and Verification Workflow

The NASA Inspection and Verification Workflow, as represented in Figure 6 below, is the process by which sanitized NASA digital media is checked and confirmed to be properly sanitized.²²

- i. The new NASA User has complied with NASA personnel security policy and procedures; and
- ii. The new NASA User has completed the required annual NASA security awareness and training policy and procedures.

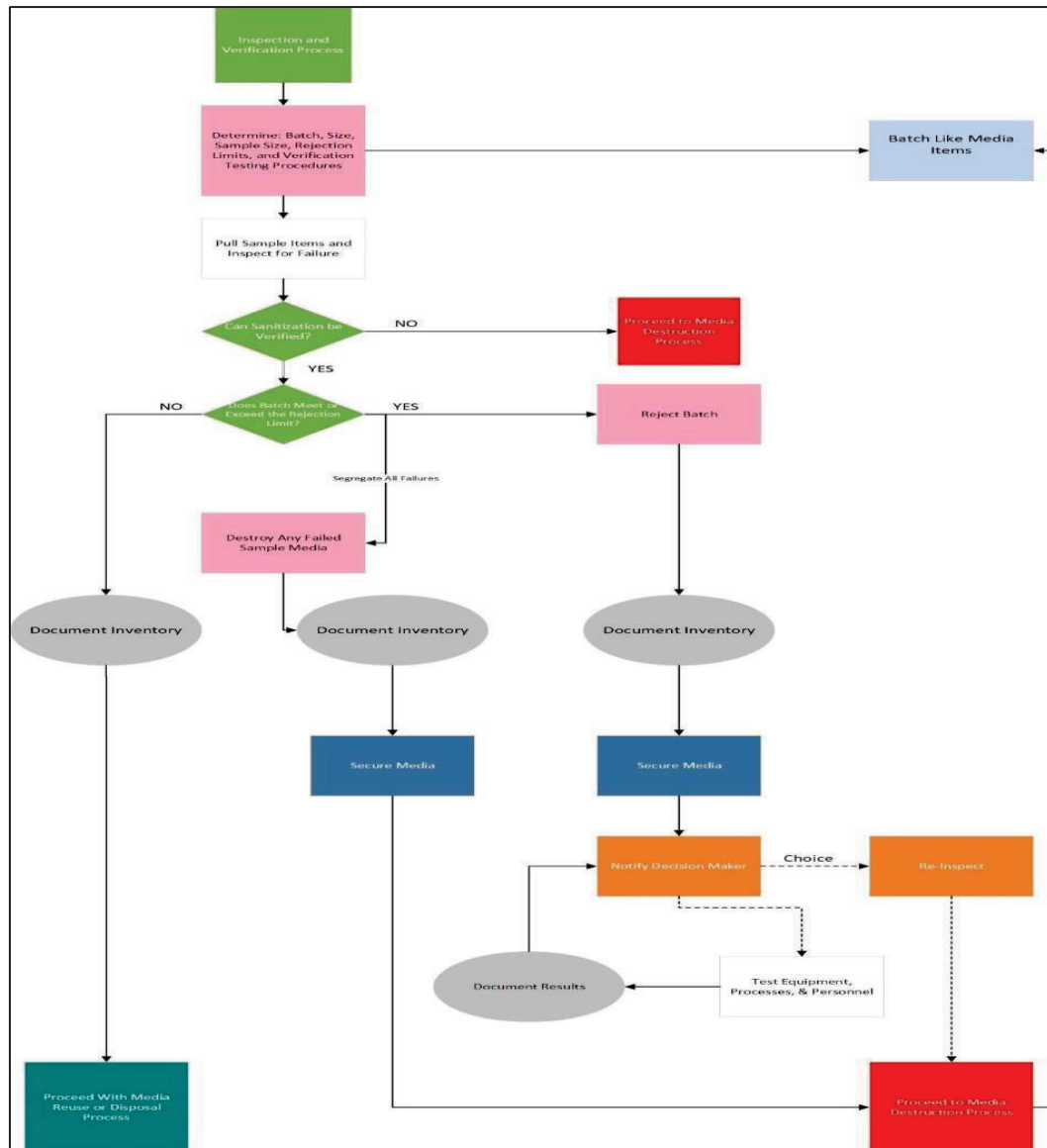


Figure 6: NASA Inspection and Verification Workflow

²² Per Section 8.5, verification of sanitization need NOT be performed if the media in question is being repurposed to an authorized IdMAX NASA User at the same or higher Sensitivity/Confidentiality level because of the following compensating IT security controls:

The person performing the inspection and verification process, the MIVP, shall not be the same person who performed the media sanitization. Additionally, the MIVP must be independent and dispassionate about the outcome of the inspection and verification process.

The MIVP makes the following determinations prior to inspecting and verifying the sanitization of digital media:

- 1) Establish requirements for verifying the successful sanitization of a population of media, using criteria from the following tables:
 - a) Table 4: 90% Confidence Level Lot/Batch Sizes, Sample Sizes and Rejection Limits, to determine the batch size of digital media to be inspected, determine sample size, and determine the rejection limits of the sample.²³
 - b) Table 5: Sanitization Verification Inspection Requirements Based on Confidentiality and Sensitivity to determine the pass/fail test needed to be performed on each digital media item in the batch sample.
- 2) Use Table 3: Good, Better, Best Approach to Selecting a Sample to determine the selection process by which they shall select the proper number of devices and conduct the tests as required.
 - a) Additionally, shall document the selection method with a justification of why the chosen method best assures that the verification sample is representative of the devices to be verified.
- 3) Make the determination if the sanitization method can be verified for the type of digital media being inspected.
 - a) If the determination is Yes, then proceed to Step 4 on this list.
 - b) If the determination is No, then proceed to the Media Destruction Process which is outlined in Section 10.
- 4) After testing²⁴ the entire sample, determine if the sample tested has met or exceeded the rejection limits of the sample (e.g. If there is one or more failure) as determined in Step 1.a.
 - a) If the determination is No, then proceed to Step 5.
 - b) If the determination is Yes, perform the functions listed in Step 7 **and** Step 8 in parallel.

²³ By using Table 4 to produce the batch size and rejection limits the MIVP is complying with the NASA CIO's commitment to verify all sanitized media to a point that is equal to, or exceeds, a 90% Confidence Level.

²⁴ As part of the verification process, the MIVP shall make every effort to closely inspect the digital media casing for any additional digital media that may reside within the device. For example, the MIVP should be looking for: Any CD/DVD or like media that may have been left in a CD tray; Any Compact Flash, SD, USB drives, or other writeable media that may not have been removed in an earlier sanitization process; or Any additional, or previously undiscovered, hard drives that may not have been removed in an earlier sanitization processes. Should any of these or any other digital media items be found during the inspection process, the MIVP shall immediately reject the batch, as described in Section 10.1.

- 5) Completely and thoroughly document the inventory information from the digital media device and collect, at minimum, the following information:
 - a) Manufacturer
 - b) Model information
 - c) Serial Number
 - d) Device Type
 - e) Media Confidentiality and Sensitivity Tag information
 - f) Any NASA organizational identification
 - g) Device location information
 - h) Device name (if applicable)
- 6) After completely and thoroughly documenting the inventory, permit the devices to proceed with any Media Reuse or Disposal Process the Agency wishes to pursue.
- 7) Ensure that any and all failed sample media devices are segregated from the batch and destroyed by following the requirements outlined in Steps 7.a-7.b.
 - a) Ensure that the inventoried media is secured in a manner that is not easily accessible to unauthorized personnel, and if required, in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable law, regulations, and government-wide policies for protecting and securing government data.
 - b) Ensure that the inventoried media are destroyed according to the Media Destruction Process which is outlined in Section 10, and proceed with requirements of Steps 8-9.
- 8) Reject the batch from which the sample was taken and proceed with requirements of Step 8.a.
 - a) Ensure that inventoried media is secured in a manner that is not easily accessible to unauthorized personnel, and if required, in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable law, regulations, and government-wide policies for protecting and securing government data.
- 9) Notify²⁵ the Center CISO when the verification process identifies one or more failures in a batch of sanitization media and that the sample failure resulted in a rejection of the batch. At such time the Center CISO may pursue one of the three options listed below:
 - a) The Center CISO may choose to test the equipment, processes, and the personnel who tested the failed batch. The Center CISO will assist the MIVP in ensuring that there were no false failures that occurred during the verification and inspection process – which may have occurred as a result of faulty equipment, improper procedures, or improperly or inadequately trained personnel. If false failures are identified, or if a true failure resulted in the failure of the batch, the Center CISO shall make corrective actions to the equipment, processes, and/or the personnel to ensure that the verification and inspection processes are functioning correctly.

²⁵ If the inspection and verification process is being conducted on devices that are owned by a contractor, but contain NASA data, the MIVP shall contact the Contract Manager, who when notified of a batch failure shall, seek and follow the direction of the Center CISO, via the COTR, to properly and securely dispose of the rejected digital media in a manner which ensures that the information it does or may contain, will not become the source of an unapproved leakage.

- b) The Center CISO documents any findings that may have been uncovered to explain why there was a rejected batch, and any corrective actions may have been taken and proceed back to Step 9.
- c) The Center CISO may choose to instruct the MIVP to void the rejection and to re-inspect the batch. This option to re-inspect a batch is only allowed to be exercised once per batch.
- d) After completely and thoroughly documenting the inventory, the MIVP gathers and sorts like media devices into a batch and re-submit the batch for inspection by following the requirements listed in Step 1.
- e) The Center CISO may choose to instruct the MIVP to ensure that the inventoried media are destroyed according to the Media Destruction Process which is outlined in Section 10.

9.2 Frequency of Inspection and Verification

Every batch of sanitized digital media shall be inspected and verified. All reasonable attempts to “sample often” shall be pursued.

Any attempts to manipulate batch sizes and/or to extend frequencies between inspections with the intent to avoid the requirement to inspect and verify media sanitization, or to reduce the amount of a required sample, shall not be permitted.

9.3 Sample Selection

The foundation of NASA’s inspection and verification process shall be predicated upon using a sample selection methodology based upon randomness. While there are multiple commonly used sample selection methods used in the IT auditing community, only the following three sample selection methods shall be authorized for inspection and verification at NASA:

- a. Random sampling,²⁶
- b. Systematic sampling,²⁷ and

²⁶ Random: Since only a purely random sample ensures that a conclusion relative to the population sampled (with a statistical level of confidence) can be asserted about that population, the random sampling method shall be the preferred method of sampling for the digital media inspection and verification process at NASA.

²⁷ Systematic: Since the uncertain starting point coupled with an unpredictable interval inserts a degree of randomness to the sampling process enabling all units in the population to have an equal chance of selection, the systematic sampling method can be employed. If this method is used, the MIVP shall ensure that both the starting point and the interval are indeed random and free from predictability or bias. However, systematic sampling is not the preferred method of sampling for the digital media inspection and verification process at NASA.

c. Haphazard sampling.²⁸

Some types of media (e.g., magnetic tapes) may require a particular sampling method not included in the list above. Table 5 in Section 9.5 describes specific sampling methods for certain media, where applicable.

Table 3 below presents a “Good, Better, Best” approach to selecting a sampling method.

Table 3: Good, Better, Best Approach to Selecting and Sampling Method

Type of Sampling	Description	Rank
Haphazard	Samples are selected from the inspection population without following a structured technique, while avoiding any conscious bias or predictability.	Good
Systematic	Sampled units are selected from the inspection population at a fixed interval, chosen at random at the outset. Effectively, this method is a matter of choosing every Nth item from the inspection population to sample, where N is a randomly chosen number.	Better
Random	All units in the inspection population have an equal chance of being sampled.	Best

²⁸ Haphazard: If the MIVP can ensure that all units in the population have an equal chance of selection without predictability, bias, or structure, the haphazard sampling method may be employed. However, a haphazard sample is not the preferred method of sampling for the digital media inspection and verification process at NASA.

9.4 Samples and Rejection Limits

Establishment of a sample size and rejection limits shall be determined based upon a 90% Confidence Level. Therefore, the selection of a sample size is determined by the lot or batch size, as outlined in Table 4 below.

Table 4: 90% Confidence Level Lot/Batch Sizes, Sample Sizes, & Rejection Limits

90% Confidence Level			
Lot or Batch Size Between		Sample Size	Rejection Limit
2	8	All	1 or More
9	15	All or At Least 12	1 or More
16	25	All or At Least 18	1 or More
26	50	All or At Least 29	1 or More
51	90	39	1 or More
91	150	47	1 or More
151	280	55	1 or More
281	500	60	1 or More
501	1,200	64	1 or More
1,201	3,200	66	1 or More
3,201	10,000	67	1 or More
10,001	35,000	68	1 or More
35,001	150,000	68	1 or More
150,001	500,000	68	1 or More
500,001	over	At Minimum 68	1 or More

Source: NASA OIG Statistician

9.5 Verification Testing Requirements

Specific sanitization Verification Testing Requirements are set out by digital media type in Table 5, below, based on the Confidentiality or Sensitivity level. For ease of use, Table 5 mirrors Section 8.5, Table 2.

Table 5: Sanitization Verification Testing Requirements Based on Confidentiality and Sensitivity

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Hand-Held Devices				
Cell Phones and PDAs that ARE NOT capable of NASA email or general Internet browsing	Please contact the manufacturer for proper sanitization verification procedures.		Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.	

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Cell and Smart Phones, PDAs, and tablet or tablet-like devices that ARE capable of NASA email or general Internet browsing	Please contact the manufacturer for proper sanitization verification procedures.			<p>Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.</p>

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Networking Devices				
Networking Devices (all types)	Please contact the manufacturer for proper sanitization verification procedures.			<p>Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding</p> <p>controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.</p>

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Office Equipment				
				<p>Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding</p>

Copy Machines	Please contact the manufacturer for proper sanitization verification procedures.	controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.
---------------	--	---

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Fax Machines	<p>Please contact the manufacturer for proper sanitization verification procedures.</p> <p>For older fax machines that use =carbon paper or a similar physical medium that retains a copy of an incoming fax, certify or witness that shredding or incineration has been performed.</p>			<p>Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.</p>
				<p>Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding</p>

Printers	Please contact the manufacturer for proper sanitization verification procedures.			controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.
	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Generic Disk Drives				
ATA and SATA Hard Drives (not including solid-state versions)	Verify sanitization by conducting a delta test of the number of files on the reimaged drive against the number of files on the applied image.	Verify sanitization by conducting a delta test of the number of files on the reimaged drive against the number of files on the applied image.		Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
SCSI, SAS, and Fibre Channel Drives	<p>If sanitization was conducted by using the Agency Approved Sanitization Tools listed in Section 7.1, Table 1, verify sanitization by conducting a delta test of the number of files on the sanitized media (ideally zero) against the number of files that were on the media before sanitization.</p>	<p>If sanitization was conducted by using the Agency Approved Sanitization Tools listed in Section 7.1, Table 1, verify sanitization by conducting a delta test of the number of files on the sanitized media (ideally zero) against the number of files that were on the media before sanitization.</p>	<p>If sanitization was conducted by using the Agency Approved Sanitization Tools listed in Section 7.1, Table 1, verify sanitization by conducting a delta test of the number of files on the sanitized media (ideally zero) against the number of files that were on the media before sanitization.</p>	<p>Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.</p>
	<p>If sanitization was conducted using a product listed as approved or acceptable to or by the NSA, pursuant to Section 7.1.2, conduct a reasonable test verify sanitization has been completed to the extent that sanitization can be verified (i.e., if a degausser was used on the device, attempt to use the device, and conduct a pass/fail test), or use a verification test procedure according to the sanitization products manufacturer's recommendations.</p>	<p>If sanitization was conducted using a product listed as approved or acceptable to by the NSA, pursuant to Section 7.1, conduct a reasonable test verify sanitization has been completed to the extent that sanitization can be verified (i.e., if a degausser was used on the device, attempt to use the device, and conduct a pass/fail test), or use a verification test procedure according to the sanitization products manufacturer's recommendations.</p>	<p>If sanitization was conducted using the Agency Approved Sanitization Tools listed in Section 7.1, Table 1, verify sanitization by conducting a delta test of the number of files on the sanitized media (ideally zero) against the number of files that were on the media before sanitization.</p>	

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Solid State Drives, including USB-based Removable Media: (a.k.a. Pen Drives, Thumb Drives, and Flash Drives). Includes HSDL and PCI-E direct-attached variants.	<p>If sanitization was conducted by using the Agency Approved Sanitization Tools listed in Section 7.1, Table 1, verify sanitization by conducting a delta test of the number of files on the sanitized media (ideally zero) against the number of files that were on the media before sanitization.</p> <p>If sanitization was conducted using a product listed as approved or acceptable to by the NSA, pursuant to Section 8.1, conduct a reasonable test verify sanitization has been completed to the extent that sanitization can be verified (i.e., if a degausser was used on the device, attempt to use the device, and conduct a pass/fail test), or use a verification test procedure according to the sanitization products manufacturer's recommendations.</p>			<p>Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.</p>

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Magnetic Disks				
Floppies	<p>If sanitization was conducted by using the Agency Approved Sanitization Tools listed in Section 7.1, Table 1, verify sanitization by conducting a delta test of the number of files on the sanitized media (ideally zero) against the number of files that were on the media before sanitization.</p> <p>If sanitization was conducted using a product listed as approved or acceptable to by the NSA, pursuant to Section 8.1, Table 1, conduct a reasonable test to verify sanitization has been completed to the extent that sanitization can be verified (i.e., if a degausser was used on the device, attempt to use the device, and conduct a pass/fail test), or use a verification test procedure according to the sanitization products manufacturer's recommendations.</p>			<p>Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.</p>

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Zip Disks	<p>If sanitization was conducted by using the Agency Approved Sanitization Tools listed in Section 7.1, Table 1, verify sanitization by conducting a delta test of the number of files on the sanitized media (ideally zero) against the number of files that were on the media before sanitization.</p> <p>If sanitization was conducted using a product listed as approved or acceptable to by the NSA, pursuant to Section 7.1, Table 1, conduct a reasonable test verify sanitization has been completed to the extent that sanitization can be verified (i.e., if a degausser was used on the device, attempt to use the device, and conduct a pass/fail test), or use a verification test procedure according to the sanitization products manufacturer's recommendations.</p>			<p>Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.</p>

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Magnetic Tapes				
Reel and Cassette Format Magnetic Tapes	<p>If the tape was sanitized using either a degaussing method or an overwriting method, verify sanitization by operating the tape in a system similar to the one that originally recorded the data, and conduct three tests each one minute long (one at the beginning, one at the end, and one at a random location) and determine if the known non-sensitive signals are executing properly and clearly for each test location. If one or more tests fail</p>			<p>Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all</p>

	this verification then reject the media.	applicable laws, regulations, and government-wide policies for protecting and securing government data.
--	--	---

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Optical Disks				
CDs/DVDs/Blue Ray	Certify that shredding has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.		Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.	
	Certify that shredding has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.			

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Internal Memory				
Compact Flash Cards/Drives, SD, Sony MemoryStick™	If sanitization was conducted by using the Agency Approved Sanitization Tools listed in Section 7.1, Table 1, verify sanitization by conducting a delta test of the number of files on the sanitized media (ideally zero) against the number of files that were on the media before sanitization.		Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government.	
	If sanitization was conducted using a product listed as approved or acceptable to use by the NSA, pursuant to Section 7.1, conduct a reasonable test verify sanitization has been completed to the extent that sanitization can be verified (i.e., if a degausser was used on the device, attempt to boot the device, and conduct a pass/fail test), or use a verification test procedure according to the sanitization products manufacturer’s recommendations.			

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Magnetic Core Memory	<p>If sanitization was conducted using the Agency Approved Sanitization Tools listed in Section 7.1, Table 1, verify sanitization by conducting a delta test of the number of files on the sanitized media (ideally zero) against the number of files that were on the media before sanitization.</p> <p>If sanitization was conducted using a product listed as approved or acceptable to use by the NSA, pursuant to Section 7.1, conduct a reasonable test verify sanitization has been completed to the extent that sanitization can be verified (i.e., if a degausser was used on the device, attempt to use the device, and conduct a pass/fail test), or use a verification test procedure according to the sanitization products manufacturer’s recommendations.</p>		Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government.	
PC Cards or Personal Computer Memory Card International Association (PCMCIA) Cards	Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.			

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Smart Cards	Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.			
Magnetic Cards				
Magnetic Cards	If sanitization was conducted using the Agency Approved Sanitization Tools listed in Section 7.1, Table 1, verify sanitization by conducting a delta test of the number of files on the sanitized media (ideally zero) against the number of files that were on the media before sanitization.		Certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.	
	If sanitization was conducted using a product listed as approved or acceptable to use by the NSA, pursuant to Section 7.1, conduct a reasonable test verify sanitization has been completed to the extent that sanitization can be verified (i.e., if a degausser was used on the device, attempt to use the device, and conduct a pass/fail test), or use a verification test procedure according to the sanitization products manufacturer’s recommendations.			
Other				

	Sanitization Verification Testing Requirements			
Media Type	N/A	Low	Moderate	High
Media types not covered above	Verify to the extent that sanitization can be verified. If the sanitization cannot be verified, then destroy the media (shred, pulverize, incinerate in a licensed incinerator) and certify that shredding, disintegration, pulverization, or incineration has been performed in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable laws, regulations, and government-wide policies for protecting and securing government data.			

10. Digital Media Destruction Process

The NASA Media Destruction Workflow, as represented by Figure 8 below, shall be the process by which NASA digital media is properly destroyed.

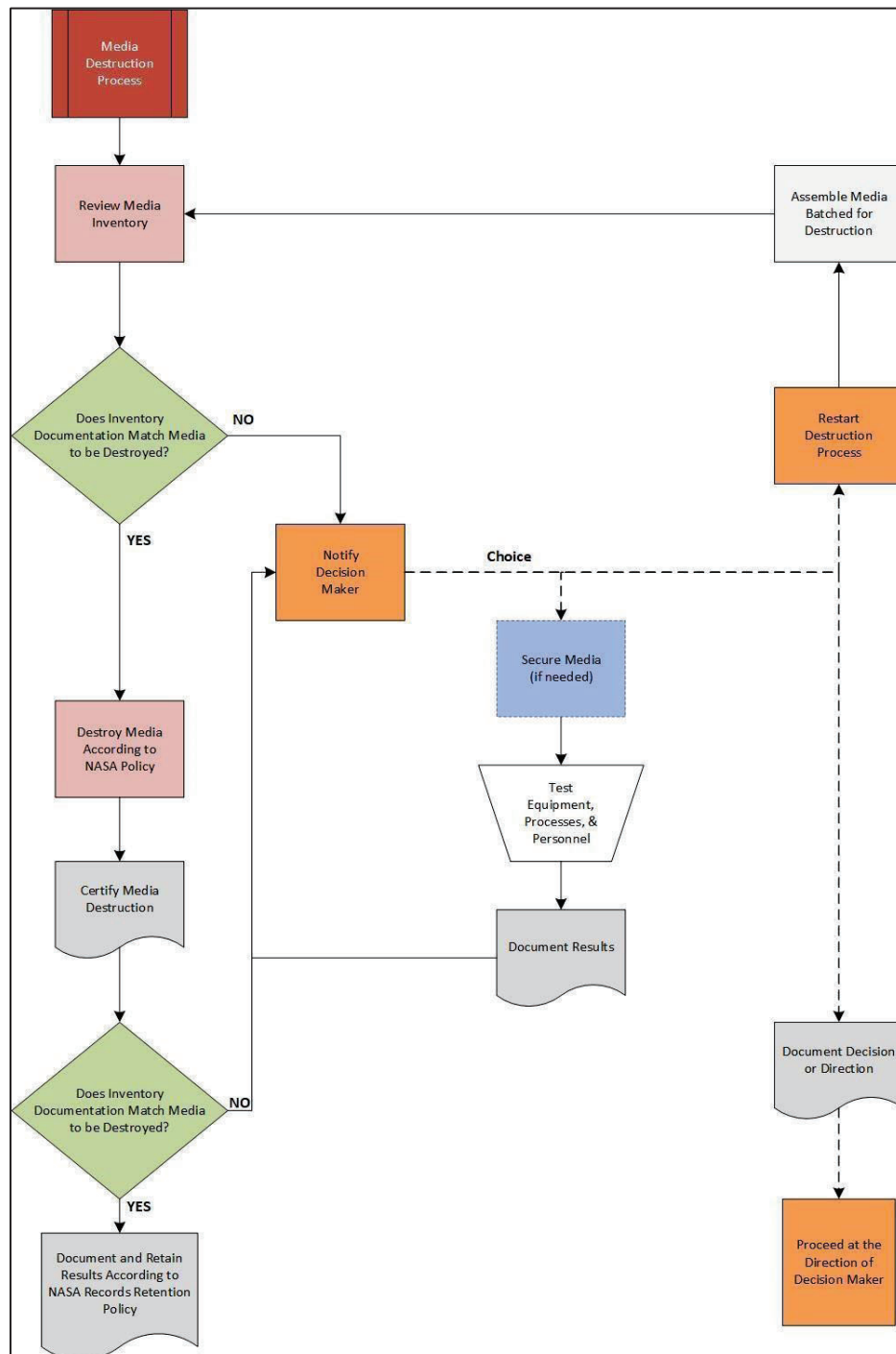


Figure 7: Media Destruction Workflow

The MSP shall review media inventory by counting the number of physical media devices in the batch and comparing that count against the previously documented inventory of the batch. Additionally, the

MSP shall compare the model information and Serial Numbers of the items contained in the batch against the previously documented inventory of the batch.

- Following a review of the media inventory, the MSP shall make the determination if the documented inventory matches the media to be destroyed.
 - If the determination is Yes, then the MSP shall proceed to “Destroy Media According to NASA Policy.”
 - If the determination is No, then the MSP shall proceed to “Notify Decision Maker.”
- The MSP shall destroy the specific media according to NASA policy, as listed in Table 2 of Section 8.5.
- The MSP shall verify (or, if unable to verify, certify) that the media was properly destroyed according to NASA policy, as listed in Table 5 of Section 10.5, and document the inventory that was destroyed.
- The MSP shall make the determination if the previously documented inventory of the batch matches the destruction certification.
 - If the determination is Yes, then the MSP shall proceed to “Document and Retain Results According to NASA’s Record Retention Policy.”
 - If the determination is No, then the MSP shall proceed to “Notify Decision Maker.”
- The MSP shall document and retain the results of the media destruction process according to the NASA records retention policy.
- The MSP²⁹ shall notify the Center CISO when the either the previously documented inventory of the batch does not match the media to be destroyed, or when the previously documented inventory of the batch does not match the destruction certification. In both instances the Center CISO may pursue one of the three options as listed below:
 - If possible, the Center CISO shall instruct the MIVP to ensure that media to be destroyed is secured in a manner that is not easily accessible to unauthorized personnel, and if required, in a manner that meets the safeguarding controls of NASA policy, or is deemed to be pursuant to and consistent with all applicable law, regulations, and government-wide policies for protecting and securing government data.
 - The Center CISO may choose to test the equipment, the processes, and the personnel which uncovered the documentation matching, or destruction anomalies. The Center CISO shall assist the MSP in ensuring that there were no false negatives that occurred during the documentation matching, or destruction process, which may have occurred as a result of faulty equipment, improper procedures, or improperly or inadequately trained personnel. If

²⁹ If the media destruction process is being conducted on devices that are owned by a contractor, but contain NASA data, the MSP shall contact the Contract Manager in lieu of the Center CISO. The Contract Manager, when notified about any inconsistency or error related to the documented inventory or destruction certification, shall seek and follow the direction of the Center CISO, via the COTR, to resolve any inconsistency or errors via the Media Destruction Process as outlined in this Handbook so as to ensure that NASA data is protected.

false negatives are identified, or if a true failure occurred in the documentation matching, or destruction process, the Center CISO shall make corrective actions to the equipment, processes, and/or the personnel to ensure that the matching and destruction processes are functioning correctly.

- The Center CISO shall document and retain any findings that may have been uncovered to explain why there was a documentation matching or destruction anomaly and document any corrective actions that were taken to avoid such anomalies in the future. When completed the Center CISO may instruct the MSP proceed to either:
 - Ensure that media to be destroyed is properly secured, as described earlier; or
 - Restart the destruction process with “Assemble Media Batched for Destruction.”
- After completely and thoroughly documenting the inventory, the MSP shall gather and assemble the media batched for destruction and re-submit the batch for review of the media inventory.
- The MSP shall document the decision or direction of the Center CISO and retain such documentation according to the NASA records retention policy.
- The MSP shall proceed at the direction of the Center CISO.

11. Exceptions to Media Sanitization Procedures

Digital media devices leaving NASA’s control solely for the purpose of warranty replacement or warranty repair shall be exempt from this policy’s requirement to destroy.

However, a best effort shall be made to ensure that media which is leaving NASA’s control for the purposes of a warranty replacement or repair is either inoperable, or the data on the device is secured in such a way as to ensure that the NASA data is not retrievable, or will not be retrieved by contractual agreement.³⁰

To reduce the risk of exposure of NASA information that is not appropriate for public release (non-public information), the NASA official submitting the digital media devices for warranty replacement or repair shall ensure that the information that the digital media device did, does, or may contain, shall not become the source of a leakage of non-public information held by NASA, NASA contractors, and/or NASA partners.

³⁰ Check with the COTR for more detailed instructions on how to ensure that NASA data leaving NASA’s control as part of a warranty replacement or warranty repair will not become the source of a leakage.

Appendix A: Examples of Information Appropriate for Public Release

Information Types	Examples
Documents Intended for General Dissemination	<ul style="list-style-type: none"> • The NASA Strategic Plan. • Strategic Plans and related documents. • Personnel locator information not covered by the Privacy Act or Freedom of Information Act (FOIA) Exemption 6.³¹ This information includes, but is not limited to home telephone numbers and home addresses. • Organizational information not covered by the Privacy Act or FOIA Exemption 6. • Directions to a Center and related information that meets the legitimate needs of the public wishing to visit our Centers. • Information intended by the Agency to assist the public in better understanding the Agency's history, organization, missions, programs, and projects. • Personal, work-related biographies may be made available on the network as long as they do not compromise any sensitive information concerning PII or any aspect of the project with which the individual may be associated.
Official Agency Web sites which provide Agency policy documents	<ul style="list-style-type: none"> • Agency policy documents via the NASA Online Directives Information System (NODIS). (Note: Some NODIS policy documents are restricted for release to individuals accessing NODIS from non-NASA web sites.)
Information released by the Agency and Center Public Affairs Offices	<ul style="list-style-type: none"> • Press releases and similar information. • Public service messages such as anti-drug campaign information.

Information Types	Examples
-------------------	----------

³¹ FOIA exemption 6 applies to personnel, medical, or similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; Information exempt from disclosure under FOIA exemption 6 includes Privacy Act records (5 U.S.C. 552a) and other PII, which is addressed in OMB memoranda and guidance. PII is described by OMB as information about an individual maintained by an agency, including education, financial transactions, medical history and criminal or employment history; it also includes information which can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, mother's maiden name or biometric records. PII shall always be designated as CUI. Specific requirements and responsibilities for protecting PII are discussed in NASA's Privacy Act Regulations (14 C.F.R. Part 1212), *NPD 1382.17*, and *NPR 1382.1*.

Official Agency Information Approved for Release	<ul style="list-style-type: none">• Information that must be made available electronically to the public per the provisions of the Electronic Freedom of Information Act.• Official Agency budget information to the level of detail approved for release by the Chief Financial Officer (CFO).• Information developed by the Agency to assist industry in doing business with NASA, including electronic commerce information that does not contain proprietary data or content sensitive information as per this document (e.g., Requests for Proposals (RFP) may be published, but offer or responses to RFPs or source selection information may not be published).• Vendor quotes as part of an electronic reverse auction.
Published Information	<ul style="list-style-type: none">• Science and engineering information and data that comply with NASA's policy for publication (see <i>NPR 2200.2</i>).• NASA Standards Program information, including official Agency engineering and information technology standards.

Appendix B: Examples of Information Not Appropriate for Public Release

Information Types	Examples
<p>Sensitive information critical to protecting NASA assets and personnel</p>	<ul style="list-style-type: none"> • Computer passwords or pass phrases. • Computer network configurations or designs. • Identification of operating systems (vendor, product, and version) used on specific servers. • Internet Protocol (IP) addresses [such as when NASA chooses to assign IPs to specific systems that provide specific services and contain specific data, or when network diagrams indicate where specific IPs, net blocks, and systems are utilized. These IP addresses would be considered sensitive and should be treated as CUI. • Telephone numbers for dial-up computer connections. • IT System capabilities (e.g., staffing levels, hours of operation) or limitations. • IT System security plans, risk analyses, system vulnerabilities, procedures, and controls methods. • IT System compromise information, including evidence data. • IT System security/auditing logs. • Names/telephone numbers that uniquely identify system administrators. • Physical security information such as key codes and cipher lock combinations and significant badging information, including pictures of NASA badges. • Internal Center maps, including labeled aerial views. • Technically-detailed schematics or drawings of utilities, networks, airfields, aircraft, and buildings. • Facility information, including detailed drawings, schematics, physical locations, staffing levels, and hours of operation. • Specific information on the composition, preparation, and storage locations or optimal use of hazardous materials, explosives, or bio-toxins. • Detailed disaster recovery plans. • Details on emergency response procedures, evacuation routes, or officials responsible for these issues. • Personnel locator information as contained in Center or Agency telephone books (e.g., mail stops or building numbers).

	<ul style="list-style-type: none"> • Internal Center policies and procedures that have unresolved content publishing issues. • Personnel locators (i.e., building and room numbers or other information which could be used to determine personnel whereabouts at a given point in time, e.g., calendar information).
	<ul style="list-style-type: none"> • Information on internal NASA-only or Center-only activities or events (e.g., picnics, symposiums), especially which specifies exact locations. • Non-work-related personal information (including links to personal web pages or resumes). • Date and time identification of security-sensitive events. • Video streaming or still images of locations where physical vulnerabilities might be exposed. • Information designated as CUI. • NASA Mission Essential Infrastructures data.
Information protected by law	<ul style="list-style-type: none"> • National security information (classified information). • Personal information prohibited from disclosure by the Privacy Act or FOIA Exemption 6. This information includes, but is not limited to, Social Security numbers, home telephone numbers, home addresses, and medical data. • PII. This includes information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. • Export-controlled information. • Technical innovations prior to release approval by patent counsel. • Proprietary information of the Government or others such as: • Information disclosing inventions and technical innovations, including software, protected under 35 U.S.C. 205 and FOIA Exemption 3, unless release is approved by Center Patent Counsel. • Trade secret information protected or prohibited from disclosure under the Trade Secrets Act (18 U.S.C 1905) or FOIA Exemption 4. • Copyrighted materials unless approved for publication by the copyright owner. • Investigative information. • Commercially-licensed software restricted in accordance with the license or agreement under which it was obtained.

	<ul style="list-style-type: none"> • Information protected by treaty or agreement. • Invention disclosures. • Source evaluation information. • Confidential financial data relating to contractors. • Other information determined non-releasable under FOIA. • ITAR/EAR.
	<ul style="list-style-type: none"> • Procurement sensitive information, such as vendor quotes (except vendor quotes as part of an electronic auction), attribution information or results, or negotiating positions.
Information protected by Government or Agency policy or regulation	<ul style="list-style-type: none"> • • NASA-developed software (unless authorized). Information characterized as “Administratively Controlled Information” (per NASA policy) or previously designated “For Official Use Only.” • Pre-decisional information such as the Agency budget prior to formal release.
Embargoed scientific, technical, launch or other mission information	<ul style="list-style-type: none"> • Launch-related information whose compromise may adversely impact safety or security.

Appendix C: Media Use Policy

“NASA-owned removable media” is defined as removable media that has been purchased by or on behalf of NASA, incorporated into a security plan, and has an identifiable ISO responsible for the device. NASA’s Removable Media Use Policy is either an information system-specific policy which has been implemented through the ISO/IO/CIO authority as described in MP-7: Media Use or, if one does not exist, the following “default” policy:

- NASA partner” is defined as a contractor, government agency, affiliate, or other similar third party with a formal agreement with NASA.
- This policy does not apply to storage media used for backups that are being performed in accordance with the information system’s formal documented backup procedure (reference the CP- 09: Information System Backup control in the SSP).
- All use of removable media must conform to applicable policy such as NPRs, including (but not limited to) responsibilities outlined in the “NASA User” responsibilities in the MP-7: Media Use control.
- Removable media owned by NASA may be used in computing devices owned by NASA, subject to any applicable restrictions (e.g., a prohibition of use of removable media on a mission system).
- Per the NASA Organization Defined Value (ODV) for control MP-7 defined in NASA-SPEC-2661, NASA restricts the use of media not issued by NASA on NASA devices. When the use of nonNASA removable media is required, such as in conjunction with a business-related conference or training session, users must consult with their Center CISO prior to use.
- Sensitive Personally Identifiable Information (PII) may not be stored on removable media.

Sensitive data, as defined by NPR 2810.7. should not be stored on removable media if possible. If necessary, limited amounts of sensitive data (other than PII) may be stored on removable media for a short period of time (e.g., moving data between computers). Policies for the protection of sensitive data must be followed, especially encryption.

Final Disposition of Media (*circle one*):

Destroyed Disposed

Reused Internally Returned to Manufacturer

Other:

Appendix E: Acronyms

AAOSI	Assistant Administrator for the Office of Strategic Infrastructure
AO	Authorizing Official
ATA	Advanced Technology Attachment
CBPL	Center Business Process Lead
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISO	[Center] Chief Information Security Officer
CNSI	Classified National Security Information
CO	Contracting Officer
COTR	Contracting Officer's Technical Representative
APM	Agency Privacy Manager
CUI	Controlled Unclassified Information
CSPD	Cyber Security and Privacy Division
DAR	Data at Rest
DBAN	Darik's Boot and Nuke
EAR	Export Administration Regulations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
HBK	Handbook
ICAM	Identity, Credential, and Access Management
IdMAX	Identity Management and Account Exchange
IO	Information Owner
ISO	Information System Owner
IT	Information Technology

ITAR	International Trafficking in Arms Regulations
ITS	Information Technology Security
LoR	Level of IT Risk
MIVP	Media Inspection and Verification Personnel
MSP	Media Sanitization Personnel
NASA	National Aeronautics and Space Administration
NID	NASA Interim Directive
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NODIS	NASA Online Directives Information System
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
NSA	National Security Agency
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OS	Operating System
PDA	Personal Digital Assistant
PDO	Property Disposal Officer
PII	Personally Identifiable Information
RFP	Request for Proposal
RISCS	Risk Information Security Compliance System
SOC	Security Operations Center
SP	Special Publication
SOC	Security Operations Center
SSP	System Security Plan

Appendix F: Definitions

CD	Compact Disc: a class of media on which data are recorded by optical means.
CD-R	Compact Disc Recordable: A CD that can be written on only once but read many times. Also known as WORM.
CD-RW	Compact Disc Read/Write: A CD that can be purged and rewritten multiple times.
Clear	To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. See comments on clear/purge convergence.
CMRR	The Center for Magnetic Recording Research (CMRR) advances the state-of-the-art in magnetic storage, and trains graduate students and postdoctoral professionals. The Center is located at the University of California, San Diego.
Data	Pieces of information from which “understandable information” is derived.
Degauss	To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive in dedicated regions of the drive in between the data sectors.
Destruction	The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive.
Digital	The binary coding scheme generally used in computer technology to represent data as binary bits (1s and 0s).
Disintegration	A physically destructive method of sanitizing media; the act of separating into component parts.
Disposal	Disposal is the act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.
DVD	Digital Video Disc – a disc the same shape and size as a CD - but the DVD has a higher density and gives the option for data to be double-sided or double-layered.
DVD+R	A write-once (read only) version of the DVD+RW optical disk from the DVD+RW Alliance.
DVD+RW	A rewritable (re-recordable) DVD disk for both movies and data from the DVD+RW Alliance.

DVD-R	A write-once (read only) DVD disk for both movies and data endorsed by the DVD Forum.
DVD-RW	A rewritable (re-recordable) DVD disk for both movies and data from the DVD Forum.
Electronic Media	General term that refers to media on which data are recorded via an electrically based process.
Erase	Process intended to render magnetically stored information irretrievable by normal means.
FIPS	Federal Information Processing Standard.
Format	Pre-established layout for data.
Hard Disk	A rigid magnetic disk fixed permanently within a drive unit and used for storing data.
High-Impact System	An information system in which at least one security objective (i.e., Confidentiality, Integrity, or Availability) is assigned a FIPS 199 potential impact value of high. [FIPS 200]
IdMAX	The Identity Management and Account Exchange (IdMAX) system is NASA's integrated and authoritative Identity, Credential, and Access Management (ICAM) system that you can use to manage NASA identities and credentials, request access to a NASA facility or system, or change your personal information.
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Incineration	A physically destructive method of sanitizing media; the act of burning completely to ashes.
Information	An instance of an information type. [FIPS 199]
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide Confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542]

Information System (Also referred to as IT System)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., Sec. 3502] (Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.) [NIST]
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [NIST]

Information Technology	Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product. IT Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Note: For additional guidance/clarification on meaning or scope of IT, please refer to the definition for “Information System” which is a “discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.”.
Information Technology (IT) System	See information system.
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation. [FIPS 199]
Low-Impact System	An information system in which all three security objectives (i.e., Confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. [FIPS 200]

Level of IT Risk (LoR)	The amount of vulnerability to NASA based on the likelihood and consequences of an adverse action through improper access or use of a physical or IT asset.
Media	Plural of medium.
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Medium	Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs.
Melting	A physically destructive method of sanitizing media; to be changed from a solid to a liquid state generally by the application of heat.

Moderate-Impact System	An information system in which at least one security objective (i.e., Confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. [FIPS 200]
NASA Information	Any knowledge that that can be communicated regardless of its physical form or a characteristic, which is owned by, produced by or for, or is under the control of NASA. [NPD 2810.1D]
National Institute of Standards and Technology Special Publication (NIST SP)	Documents published by the Information Technology Lab (ITL) at NIST. Special Publications series include the 500 series (Information Technology), the 800 series (Computer Security), and the 881 series (Federal Electronic Data Interchange [EDI] Conventions). The NIST 800 Series is a set of documents that describe United States federal government computer security policies, procedures and guidelines.
Non-Public Information	Information that is not approved or appropriate for release to the public, such as (but not limited to) Personally Identifiable Information or information protected by export regulations.
Optical Disks	A plastic disk that is “written” (encoded) and “read” using an optical laser device. The disc contains a highly reflective metal and uses bits to represent data by containing areas that reduce the effect of reflection when illuminated with a narrow-beam source, such as a laser diode.
Overwrite	Writing patterns of data on top of the data stored on a magnetic medium. NSA has researched that one overwrite is good enough to sanitize most drives. See comments on clear/purge convergence.

Personal Computer Memory Card International Association (PCMCIA) Card	The Personal Computer Memory Card International Association (PCMCIA) was organized in 1989 to promote standards for both memory and I/O integrated circuit cards. PCMCIA card is a credit card-size memory or I/O device that connects to a personal computer, usually a notebook or laptop computer. Probably the most common example of a PCMCIA card is the 28.8 Kbps modem for notebook computers.
Personal Digital Assistant	The term PDA can be used for any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy. The Blackberry and Palm Pilot are examples of PDAs.
Physical Destruction	A sanitization method for optical media, such as CDs.
Pulverization	A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

Purge	Rendering sanitized data unrecoverable by laboratory attack methods. See comments on clear/purge convergence.
Read	Fundamental process in an information system that results only in the flow of information from an object to a subject.
Record	To write data on a medium, such as a magnetic tape, magnetic disk, or optical disc.
Recovery Procedures (recoverable)	Action necessary to store data files of an information system and computational capability after a system failure.
Rejection Limit	The minimum number of failures that are permitted that in a sample before rejecting the batch.
Remanence	Residual information remaining on storage media after clearing.
Removable Media	Portable digital storage media such as magnetic, optical, and solid state devices, which can be inserted into and removed from a computing device, that is used to store text, video, audio, and image information. Examples include hard disks, floppy disks, zip drives, compact disks, thumb drives, pen drives, and similar USB storage devices.
Residue	Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place.

ROM	Read Only Memory. Generally a commercially available disc or solid state device on which the content was recorded during the manufacturing process.
Sanitization	Sanitization is the process of removing data from storage devices with a degree of certainty that corresponds to the risk levels incorporated in the FIPS-199 Confidentiality categorization. The higher the Confidentiality categorization, the more assurance is necessary that information is sanitized commensurate with the potential harm that could result from its unauthorized disclosure. Thus High Sensitivity, High Confidentiality information must be impossible or nearly impossible to recover.
Secure Erase	An overwrite technology using firmware based process to overwrite a hard drive. SecureErase is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside drive hardware. It completes in about 1/8 the time of 5220 block erasure. For ATA drives manufactured after 2001 (Over 15 GB) have the Secure Erase command and successfully pass secure erase validation testing at CMRR. A standardized internal secure erase command also exists for SCSI drives, but it is optional and not currently implemented in SCSI drives tested by CMRR. SCSI drives are a small percentage of the world's hard disk drives, and the command will be implemented when users demand it.
Security	Security is a system property. Security is much more than a set of functions and mechanisms. Information technology security is a system characteristic as well as a set of mechanisms, which span the system both logically and physically.
Sensitive Information	Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. With the exception of certain types of information required to be protected by statute or in accordance with an agreement with the information owner (e.g., Limited Rights Data obtained from a contractor), the designation of information as "Sensitive but Unclassified" is largely discretionary and must be made based on sound judgment and criteria.
Shred	A method of sanitizing media; the act of cutting or tearing into small particles.
Solid State Drive	A digital media storage device using entirely non-volatile memory components for storage, such as NAND- based flash memory. Differentiated from "normal" drives that have one or more spinning storage platters.

Storage	Retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements (media) into which data may be entered, and from which data may be retrieved.
WORM	Write-Once Read Many.
Write	Fundamental operations of an information system that results only in the flow of information from a subject to an object.