DoD Supply Company Media Sanitization Procedure

Last Updated: *December 2021*

1. Purpose

The purpose of this procedure is to ensure all information assets owned by DoD Supply Company containing proprietary or Federal Contract Information (FCI) data are sanitized or destroyed prior to disposal or reuse.

2. Scope

This policy applies to all of DoD Supply Company assets storing data under the following categories:

- Government/Federal Contract Data (FCI) Data
- DoD Supply Company Proprietary Data
- DoD Supply Company Customer Data

3. Roles and Responsibilities

Role	Responsibility
CISO	• Review Procedures to ensure compliance with Policy
IT Department Personnel	• Utilize procedure(s) • Suggest any updates to procedures to the IT Manager
All Personnel	• Utilize procedure(s)

4. Procedures

General Requirements

- Per the CMMC Self-Assessment Guide – Level 1; "Media" refers to a broad range of items that store information, including paper documents, disks, tapes, digital photography, USB drives, CDs, DVDs, and mobile phones. The following procedures will outline the steps taken for DoD Supply Company staff to ensure media is sanitized or destroyed prior to disposal or reuse. All Company information systems assets will be treated as **Company Proprietary, Customer Data,** or **U.S. Government FCI** as specified in table 1.

- If there is **Company Proprietary, Customer Data,** or **U.S. Government/ FCI** data, authorized employees and/or IT Department Staff should either:

  - shred or destroy the device before disposal so it cannot be read; or
  - clean or purge the information if you want to reuse the device.

Table 1 Data Categorization

Data Type	Categorization
Emails	Proprietary/FCI
Inventory Data	Proprietary
Contracts	Proprietary
Contracts (Government)	FCI

4.1 Procedures for Sanitization

Information Systems containing data

- All DoD Supply Company information systems containing digital (electronic) Company Proprietary, Customer Data, or U.S. Government FCI data will be purged or destroyed using methods outlined in NIST SP 800-88:

  - Media device for reuse will be purged IAW the minimum requirements in Appendix A of NIST SP 800-88. All devices/systems media will be turned into the IT department and purge according to specific retirements for the device/media.
  - Media device for disposal will be destroyed IAW the minimum requirements in Appendix A of NIST SP 800-88. All devices/systems media will be turned into the IT department and purge according to specific retirements for the device/media.

Paper documents containing data

- All DoD Supply Company personnel will destroy paper media containing digital (physical) Company Proprietary, Customer Data, or U.S. Government FCI data will using methods outlined in NIST SP 800-88:

  - Hard Copy Storage (paper media) will be destroyed IAW the minimum requirements in Appendix A, table A-1 of NIST SP 800-88.

4.2 Documenting Device and Media Destruction

DoD Supply Company IT Department device and media sanitization documentation

All devices and systems media will be destroyed and documented IAW paragraph 4.8 of NIST SP 800-88. The DoD Supply Company IT Department will keep an inventory of devices and ensure that certificates of sanitization include the details listed in paragraph 4.8 of NIST SP 800-88. The sanitization certificate will include the following:

- Manufacturer
- Model
- Serial Number
- Organizationally Assigned Media or Property Number (if applicable)
- Media Type (i.e., magnetic, flash memory, hybrid, etc.)
- Media Source (i.e., user or computer the media came from)
- Pre-Sanitization Confidentiality Categorization (optional)
- Sanitization Description (i.e., Clear, Purge, Destroy)
- Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.)
- Tool Used (including version)
- Verification Method (i.e., full, quick sampling, etc.)
- Post-Sanitization Confidentiality Categorization (optional)
- Post-Sanitization Destination (if known)
- For Both Sanitization and Verification:
- Name of Person
- Position/Title of Person
- Date
- Location
- Phone or Other Contact Information
- Signature

3rd Party device and media destruction documentation

- All devices and systems media sent to 3rd party vendors for destruction will be documented IAW paragraph 4.8 of NIST SP 800-88. The DoD Supply Company IT Department will keep an inventory of devices and media sent for destruction. The 3rd party vendor will ensure that certificates of sanitization include the details listed in paragraph 4.8 of NIST SP 800-88. An example certificate can be found in:

  - Appendix G – Sample “Certificate of Sanitization” form

5. Personnel Authorized

Personnel Trained and Authorized

The following personnel have been trained and are authorized to conduct media sanitization or purging procedures IAW the above guidance:

Table 2 Authorized Personnel

Name	Department
Sally Sanitize	IT Department
Marty Media	IT Department
Dwayne Degauss	IT Department
Betty Whatever	HR Department

6. Compliance

General Compliance

The IT department manager will ensure that the processes and procedures listed above are applied consistently when conducting media sanitization on all systems throughout the DoD Supply Company, Headquarters (HQ), host units, and supporting units.

7. Exceptions

Any exception to the procedures must be documented and approved by the IT Manager.

Enforcement

The Infosec team will utilize the procures listed above to ensure all company and government data have been sanitized prior to the disposal of any DoD Supply Company assets. Failure to comply with these procedures can result in actions addressed under the IT Personnel requirements section in the DoD Supply Company, IT Management Policy.

8. Revision History

The revision history shall be maintained to ensure procures remain relevant and compliant. Each published update shall be recorded. Full revisions (1.0) are considered a complete reissuance of the policy and are greater than or equal to 10% of the document. Partial revision (1.1) is considered minor corrections and don’t require reissuance.

Revision History:

Version Number	Change criteria	Date
1.0	Initial document created	1/16/21
1.1	Updated procedures to reflect CMMC changes	12/22/21