State of Louisiana
Office of Technology Services

IT STD 1-17

Data Sanitization – Standards and Requirements

Explanation

Data sanitization is the process of deliberately, permanently, and irreversibly removing or destroying data stored on a device or electronic media. A device that has been successfully sanitized has no residual data even when data recovery is attempted with advanced forensic tools.

Purpose

This document empowers all applicable entities with a clear list of acceptable methods, options, and the corresponding instructions to produce consistently reliable results when Data Sanitization is required.

Approved Data Sanitization methods are listed where available and only apply to the assigned media type in the *Process Requirements* section. The sanitization procedure selected should be the option that best suits the operational needs of the agency or entity.

Scope

Any electronic device or media owned, managed, leased or utilized by the in scope agencies, as defined in IT POL 1-04 Data Sanitization Policy, with the ability to store, process, or transmit Internal, Confidential, or Restricted Data (See IT POL 1-26 Data Classification Policy). Examples include, but not limited to, Hard Drives, CDs, Backup Tapes, USB Drives, Smart Phones, Tablets, Fax Machines, Routers, Network Storage Devices, and Printers.

The following requirements should also be referenced when specifying Data Sanitization requirements for contracted partners or service providers storing or processing state data.

Sanitization Requirements

There are only three acceptable approaches for data sanitization: Clearing, Purging, and Destruction. Each method has its own requirements, considerations, and approved methods:

- **Destruction**
  Approved methods:
  - Shred (Printed Material Only – see *Approved Processes*)
  - Pulverize
  - Melt
  - Incinerate or Disintegrate

  Additional Requirements:
  - Sanitization Log (see *Log Requirements*)
  - Use of an approved process or partner
- **Purging**
  Approved methods:
  - Degaussing

  Additional Requirements:
  - Sanitization Log (see *Log Requirements*)
  - Use of approved and serviced equipment
- **Clearing**
  Approved methods:
  - Overwrite (Single or Multiple Pass)
  - Factory Reset
  - Removing Power

  Additional Requirements:
  - Sanitization Log (see *Log Requirements*)
  - Only approved procedures and software are to be used (see *Process Requirements*)
  - Overwrite Procedures must be documented, validated, and approved prior to Agency use on production equipment

See Process Requirements section
to follow the required sanitization process for specific Device or Media type

Log Requirements

Each time Data Sanitization is attempted (success or failure) a Sanitization Log Record must be created.

Each Sanitization Log Record must contain the following fields of information:

- **Media or Device Type**
- **Sanitization Status Code** (see *Approved Process section* below)
- **Manufacturer unique ID** (Ex. Hard drive Serial Number)
- **Date and Time of Sanitization**
- **Full Name of individual that performed the sanitization**

Sanitization Logs may be created and maintained manually or by an application or system.

If an Agency or entity does not have a preferred Sanitization Log format, the attached Sanitization Log should be used.

When preparing equipment for Louisiana Property Assistance Agency (LPAA) surplus or disposal, the LPAA Sanitization Certificate form should be used in place of the OTS Sanitization Log. (See LPAA POL 201401)

*In cases where an approved Third Party or Partner is performing the sanitization process, the "Sanitization Status Code" may be substituted for "Sanitization Method" and "Status" (Success or Failure).

Please contact OTS Information Security with any questions related to Third Party sanitization.

Process Requirements

Each known device or media type is listed below with the steps required to ensure all data has been removed prior to disposal or surplus.

Following each process will produce a "Sanitization Status Code" required for the Sanitization Log.

Prior to any sanitization actions the following considerations should be made:

- **Data Retention Requirements**
  Agency staff should ensure that performing data sanitization does not violate any Agency directive or legal obligation to retain data. (Ex. "Legal hold")

- **Work Area**
  Ensure individuals performing the sanitization have an organized and controlled work area to ensure devices or media are not accidently mixed with similar production devices or media.

- **Inventory**
  If bulk sanitization is required, an initial inventory should be taken (and updated as needed) of the devices or media to ensure all devices or media are accounted for throughout the sanitization process.

  Once sanitization is complete, a final count should be completed to confirm that all devices or media are accounted for and have been successfully sanitized.

Approved Processes

If an Agency, entity, or OTS resource identifies a device or media type not listed below, please contact OTS Information Security to request guidance for approved sanitization process. Please make sure to include manufacture, description, and explanation of the device or media function in a specific business process.

- **Hard Copies -** (Printed Material)
  All Printed Material containing Confidential or Restricted Data must be destroyed using one of the following specifically approved destruction methods:
  - Shred
    - Using cross cut shredders which produce particles that are 1 x 5 millimeters in size (or smaller)
  - Pulverize or Disintegrate
    - Using disintegrator devices equipped with 3/32 inch security screen
  - Incinerate (Burn)
    - Material residue must be reduced to white ash

- **CD, DVD, or BD -** (Optical Media)
  For all Optical Media Discs:
  - Destroy disc using approved destruction methods (see Sanitization Requirements)
  - Create Sanitization Log Record
  - Sanitization Status Code: **OMDS**

- **Desktop or Laptop -** (Workstations)
  Any:
  - Workstation joined to a state domain or allowed a user logon
  - Test workstation or "Lab equipment" used to process, store, or transmit any state data

  For devices containing a single Hard Disk Drive (HDD) or Solid State Drive (SSD):
  - **Use HDD or SSD process below**

  For devices containing multiple internal HDDs or SSDs:
  - Extract each drive
  - **Use HDD or SSD process below**

  For Instances where the drive will be extract from the workstation and reused, however the workstation will be disposed of or surplus:
  - Extract drive(s)
  - Label Device for Surplus (if applicable)
  - Sanitization Code: **RD**
  - **Please note**: A sanitization log entry will still be required once there is a need to sanitize the exacted drive(s).

Approved Processes (Cont.)

- **Fax Machine -** (Facsimile)
  For working devices that only perform facsimile functions:
  - Power on device and perform a factory reset via menu or manufacture instructions.
  - If completed successfully, label device with LPAA label
    - Create Sanitization Log Record
    - Sanitization Status Code: **MRS**
  - If the device does not have a reset option or does not complete the reset successfully,
    - **Follow process for broken device (below)**

  For broken devices that only perform facsimile functions:
  - Destroy Device using approved destruction methods (see Sanitization Requirements)
  - Create Sanitization Log Record
  - Sanitization Status Code: **DS**

  For devices that perform fax, printer, and coping functions:
  - **Use Multifunction Device (MFD) process below**

- **Printer, Scanner, Copy Machine, or Multifunction Device (MFD)** - (Office Equipment)
  For devices containing a Hard Disk Drive (HDD) or Solid State Drive (SSD):
  - **Use HDD or SSD process below**

  For operational devices that do not contain HDD or SSD internal storage:
  - Contact manufacturer (by email, phone, or website) for the steps required to clear all data for the specific device model
  - If completed successfully, label device with LPAA label
    - Create Sanitization Log Record
    - Sanitization Status Code: **MRS**

  For working or broken devices that do not store or cache data:
  - Label device with LPAA label
  - Create Sanitization Log Record
  - Sanitization Status Code: **ND**

  For broken or damaged devices that have been confirmed to or expected to store or cache data:
  - Destroy Device using approved destruction methods (see *Sanitization Requirements*)
  - Create Sanitization Log Record
  - Sanitization Status Code: **DS**

Approved Processes (Cont.)

- **Smart Phone, Tablet, or PDA** (Ex. iPhone, Blackberry, iPad, etc.) – (Mobile Devices)
  For operational devices:
    - Perform Full System Reset or contact manufacturer (by email, phone, or website) for the steps required to perform a FULL factory reset
    - If reset completed successfully:
        - Manually spot check device to ensure all photos, documents, history was successfully removed
        - Label device with LPAA label
        - Create Sanitization Log Record
        - Sanitization Status Code: **MRS**
    - If reset failed:
        - Create Sanitization Log Record
        - Sanitization Status Code: **MRFMD**
        - **Follow process for broken or damaged device**
    - If reset is not available:
        - **Follow process for broken or damaged device**

  For broken or damaged devices:
    - Destroy device using approved destruction methods (see *Sanitization Requirements*).
    - Create Sanitization Log Record.
    - Sanitization Status Code: **DS**

- **Firewall, Router, or Voice Over IP Handset -** (Network Devices)
  For operational devices:
    - Contact manufacturer (by email, phone, or website) for the steps required to perform a factory reset
    - If reset completed successfully:
        - Label device with LPAA label
        - Create Sanitization Log Record
        - Sanitization Status Code: **MRS**
    - If reset failed:
        - Create Sanitization Log Record
        - Sanitization Status Code: **MRFMD**
        - **Follow process for broken or damaged device**
    - If reset is not available:
        - **Follow process for broken or damaged device**

  For broken or damaged devices:
    - Destroy device using approved destruction methods (see *Sanitization Requirements*)
    - Create Sanitization Log Record
    - Sanitization Status Code: **DS**

- **Portable USB Drives or Memory Cards -** (Removable Media)
  For all:
    - Destroy disc using approved destruction methods (see *Sanitization Requirements*)
    - Create Sanitization Log Record
    - Sanitization Status Code: **RMDS**

Approved Processes (Cont.)

- **Hard Disk Drives** - (HDD) **or Solid State Drives** - (SSD) - SCSI, IDE & ATA (SATA, eSATA)
  For an operational drive:
  - An approved OTS Overwrite Standard Operating Procedure (SOP) must be followed:
    - IT SOP 1-01 Drive Overwrite Procedure – (Single Pass)
    - IT SOP 1-02 Drive Overwrite Procedure – (Triple Pass)
  - **If an Agency or OTS resource prefers to utilize an alternate Overwrite procedure or solution**:
    - The alternate procedure must be documented (see OTS SOP format)
    - The proposed procedure must be sent to OTS Information Security for review and approval
    - Written approval must be obtained from OTS Information Security prior to utilizing any alternative overwrite procedures or solutions for sanitizing any production drives
  - If an approved overwrite procedure completed successfully:
    - If applicable, make sure to correctly place drive back in the correct parent device
    - Label device with LPAA label
    - Create Sanitization Log Record
    - Sanitization Status Code: **OWS**
  - If approved overwrite procedure failed:
    - Create Sanitization Log Record
    - Sanitization Status Code: **OWFMD**
    - **Follow process for damaged or inoperable drive**

  For a damaged or inoperable drive:
  - If HDD:
    - The drive may be degaussed (if equipment is available) or destroyed.
    - If Degaussing is preferred:
      - □ Degauss
      - □ Create Sanitization Log Record
      - □ Sanitization Status Code: **OWFDGS**
      - □ Label original (parent) device with LPAA label
    - If Destruction is required:
      - □ Destroy drive using approved destruction methods (see *Sanitization Requirements*).
      - □ Create Sanitization Log Record.
      - □ Sanitization Status Code: **OWFDS**
      - □ Label original (parent) device with LPAA label.
  - If SSD:
    - Destroy drive using approved destruction methods (see *Sanitization Requirements*)
    - Create Sanitization Log Record
    - Sanitization Status Code: **OWFDS**
    - Label original (parent) device with LPAA label

Approved Processes (Cont.)

- **Backup Tapes -** (Magnetic Tape)
  For all:
  - If degausser is available:
    - Degauss
    - Create Sanitization Log Record
    - Sanitization Status Code: **DGS**
  - If degausser is not available:
    - Destroy tape using approved destruction methods (see *Sanitization Requirements*)
    - Create Sanitization Log Record
    - Sanitization Status Code: **DS**

- **Server or Network Storage**
  For all:
  - Remove each individual storage drive
  - **Follow process for HDD**
  - If an alternative approach is preferred:
    - Document alternative approach
    - Send to OTS Information Security for review and approval
    - Written approval must be obtained from OTS Information Security prior to performing any alternative procedures or solutions for sanitizing any server or network storage

- **DRAM, SRAM, or NOVRAM –** (RAM)
  For all:
  - Remove power or battery for a minimum of 5 minutes
  - Create Sanitization Log Record
  - Sanitization Status Code: **PRS**

- **EAPROM, EEPROM, or EPROM –** (ROM)
  For all:
  - Destroy media using approved destruction methods (see *Sanitization Requirements*)
  - Create Sanitization Log Record
  - Sanitization Status Code: **DS**

Sanitization Status Codes

To ease any review process; below is a mapping of devices or media type to potential code and includes Sanitization Method and Status translation.

Media Type	Code	Method	Status	Condition
Office Equipment	ND	N/A	No Data	Reusable
Workstation	RD	Drive Removed	No Data	Reusable
HDD, SSD	OWS	Overwrite	Success	Reusable
Facsimile, Office Equipment, Network Device, Mobile Device	MRS	Reset	Success	Reusable
RAM	PRS	Removed Power	Success	Reusable
HDD	OWFD	Overwrite	Failure – Marked for Degaussing	Not Reusable
HDD, SSD	OWFMD	Overwrite	Failure – Marked for Destruction	Not Reusable
Network Device, Mobile Device	MRFMD	Reset	Failure – Marked for Destruction	Not Reusable
Facsimile, Office Equipment, Network Device, Mobile Device, Magnetic Tape, ROM	DS	Destruction	Success	Not Reusable
HDD, SSD	OWFDS	Destruction	Success	Not Reusable
HDD, Magnetic Tape	DGS	Degaussed	Success	Not Reusable
Optical Media	OMDS	Destruction	Success	Not Reusable
Removable Media	RMDS	Destruction	Success	Not Reusable

Related Policies, Standards, Procedures
IT POL 1-26 Data Classification Policy
IT POL 1-04 Data Sanitization Policy
IT SOP 1-01 Drive Overwrite – (Single Pass)
IT SOP 1-02 Drive Overwrite – (Triple Pass)
LPAA POL 201401

Owner
Division of Administration, Office of Technology Services, Information Security

Contact Information
OTS Information Security: security@la.gov

Effective Date
12/08/2014

Revision History

Date	Author	Description
10/21/2014	Ivory Junius	Creation
12/08/2014	Dustin Glover	Content and Format Revision
02/05/2015	Dustin Glover	• Status Code added, Drive Removal for Workstations • Removed verbiage causing potential confusion for operational Printers that do not store data • Changes\Improvements Document format

Authorization

Richard Howze

Richard "Dickie" Howze, State Chief Information Officer