Data Sanitization Policy and Procedures

Regulatory Compliance

Office of Technology Services
Information Security and Compliance

State of Louisiana

Revision: 1.03
Date: October 28, 2024

Table of Contents

Overview

Data sanitization is the process of deliberately, permanently, and irreversibly removing or destroying data stored on a device or electronic media. The techniques outlined in this document serve to ensure the confidentiality of sensitive data is maintained while minimizing the risk of unauthorized disclosure of information. A device that has been successfully sanitized has no residual data even when data recovery is attempted with advanced forensic tools. Data sanitization is required when a device reaches end-of-life or is being reused outside of its original purpose.

Purpose

The purpose of this document is to establish a framework for all applicable entities on the OTS approved methods for media sanitization, in accordance with NIST SP 800-88 Rev. 1 - Guidelines for Media Sanitization. The policy is broken down by media type and data type, to produce consistently reliable results. Once media type and data type are determined, the sanitization procedure selected should be the option that best suits the operational needs of the Agency or entity.

The procedures included in the Process Requirements section are to ensure storage devices containing Confidential or Restricted data, as defined in the Office of Technology Services (OTS) Information Security Policy (ISP), are sanitized thoroughly using either a single pass overwrite method or a separate triple pass procedure (as required for Criminal Justice Information Systems (CJIS) data and others).

Scope

This policy and procedures apply to all storage devices and media, including but not limited to hard drives, SSDs, tapes, USB drives, and any other digital storage, as defined in the OTS Information Security Policy (ISP), which have the capability to store, process, or transmit Internal, Confidential, or Restricted data (refer to the Data Classification Levels section of the ISP). These standards are mandatory for all devices or media managed, leased, or owned by OTS or in-scope agencies. Examples of applicable devices include but are not limited to hard drives, CDs, backup tapes, USB drives, smartphones, tablets, fax machines, routers, network storage devices, and printers. Furthermore, these requirements must be followed when specifying data sanitization requirements for contracted partners or service providers who store or process state data.

The Chief Information Security Officer (CISO) or a designated representative will conduct an annual review of this document to ensure compliance with state and federal regulations and security safeguards. Furthermore, the document will be updated at least every three (3) years, or whenever there is a significant change or security event.

Roles and Responsibilities

- Information Security Team (IST): Responsible for ensuring data sanitization activities are compliant with system security policies, procedures, and standards.
- Property Manager: Designated agency official responsible for requesting sanitization. Must ensure assets deemed to be electronic media do not include assets of any other class.

- OTS Technician: Responsible for performing and/or monitoring data sanitization activities.
- OTS Supervisor: Responsible for reviewing and approving data sanitization activities.
- System Owners: Responsible for ensuring all data sanitization activities have been authorized and documented.
- Third-Party Vendors: Required to adhere to security and privacy controls as specified in contracts and service-level agreements (SLAs).

Policy and Procedures

Sanitization Requirements

Per NIST Special Publication 800-88, Rev. 1, the three (3) acceptable methods for data sanitization are: clearing, purging, and destruction. Each method of data sanitization has its own requirements, considerations, and approved procedures to ensure all data is irretrievable. See Process Requirements section to follow required data sanitization process for specific device and media types.

Clearing

Approved Methods:

- Overwrite (single or multiple pass)
- Factory Reset
- Removing Power

Additional Requirements:

- Sanitization Log (See Log Requirements section.)
- Only approved procedures and software are to be used (See Process Requirements section.)
- Overwrite Procedures must be documented, validated, and approved prior to Agency use on production Equipment

Purging

Approved Methods:

- Degaussing

Additional Requirements:

- Sanitization Log (See Log Requirements section.)
- Use of approved and serviced equipment

Destruction

Approved methods:

- Shred (Printed Material Only – See Approved Processes section.)
- Pulverize
- Melt
- Incinerate or Disintegrate

Additional Requirements:

- Sanitization Log (See Log Requirements section.)
- Use of approved process or partner

Log Requirements

When preparing equipment for Louisiana Property Assistance Agency (LPAA) surplus or disposal, the LPPA Certificate of Data Sanitization Form must be used. (See LPAA POL 201401). The following fields are contained within the Certificate of Data Sanitization and must be completed accurately:

- Asset Number
- Asset Description
- Serial Number or Manufacturer unique ID
- Media Type
- Data Sanitization Status Code (See Approved Process section.)
- Printed full name and signature of individual performing sanitization
- Last 4 digits of social security number
- Date of sanitization

Once the Certificate of Data Sanitization is completed by the OTS technician performing the sanitization, the form must be forwarded to the individual's OTS supervisor, who is required to:

- Review
- Approve the document with printed full name, signature, and date to affirm the work has been completed.
- Confirm the agency Property Manager's adds printed full name, signature, date, Agency Number and Transfer Number to the Certificate of Data Sanitization.

The OTS technician who performed the sanitization must then:

- Verify the Certificate of Data Sanitization has been electronically attached to the request for LPAA to consider approval.
- Ensure the original Certificate of Data Sanitization has been returned to the agency for retention.

NOTE: If an Agency wishes to use another form to meet the sanitization log requirement, prior approval must be obtained from LPAA's Compliance Supervisor. For example, Form G is an approved, Louisiana Department of Health specific version of the Certificate of Data Sanitization.

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 IST 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 must be made:

- Data Retention Requirements. Agency staff must provide the required data retention duration and ensure that performing the data sanitization does not violate any Agency directive, regulatory requirement or legal obligation to retain data. (e.g., "Legal hold")
- Work Area. Individuals performing sanitization must have an organized and controlled work area to ensure devices or media remain separate from similar production devices or media. A dedicated workspace lowers the risk of unintended data loss resulting from accidental selection of the wrong equipment to be sanitized.
- 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.
- Authorized Access. Individuals conducting the sanitization process must be authorized and approved for access to the specific type of data being sanitized. If an individual is not authorized or approved for that data type, they must be accompanied by authorized personnel at all times during the sanitization. For example, the sanitization of Restricted data by a third party, without prior approval for unescorted access, must occur on-site and under the supervision of authorized staff.

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

Approved Processes

Approved data sanitization methods apply to the assigned media types that follow. If an Agency, entity, or OTS resource identifies a device or media type that is not listed below, please contact IST to request guidance for approved sanitization process. Please make sure to include manufacturer, 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 the Shred destruction method:

- Using cross cut shredders which produce particles that are 1x5 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 Blu-ray Disk (BD) - (Optical Media)

For all Optical Media Discs:

- Destroy disc using approved destruction methods (See Sanitization Requirements section.)
- Create Certificate of Data Sanitization
- Sanitization Status Code: Optical Media Destruction Successful (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 HDD or SSD:

- Extract each drive
- Use HDD or SSD process below

For instances where the drive must be extracted from the workstation and reused, however the workstation will be disposed of or surplus:

- Extract drive(s)
- Label Device for Surplus (if applicable)
- Sanitization Status Code: Removed Drive (RD)

NOTE: A Certificate of Data Sanitization entry will still be required once there is a need to sanitize the extracted drive(s).

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:
    - Affix an LPAA Data Sanitization Label to the device
    - Create Certificate of Data Sanitization
    - Sanitization Status Code: Machine Reset Successful (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 section.)
- Create Certificate of Data Sanitization
- Sanitization Status Code: Destruction Successful (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 an HDD or 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:

- Affix an LPAA Data Sanitization Label to the device
- Create Certificate of Data Sanitization
- Sanitization Status Code: MRS

For working or broken devices that do not store or cache data:

- Affix an LPAA Data Sanitization Label to the device
- Create Certificate of Data Sanitization
- Sanitization Status Code: No Drive (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 section.)
- Create Certificate of Data Sanitization
- Sanitization Status Code: DS

Smart Phone, Tablet, or PDA (e.g., 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
- Affix an LPAA Data Sanitization Label to the device
- Complete Certificate of Data Sanitization
- Sanitization Status Code: MRS

If reset failed:

- Complete Certificate of Data Sanitization
- Sanitization Status Code: Machine Reset Failure/Marked for Destruction (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 section.)
- Complete Certificate of Data Sanitization
- 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:

- Affix LPAA Data Sanitization label to the device
- Complete Certificate of Data Sanitization

- Sanitization Status Code: MRS

If reset failed:
- Complete Certificate of Data Sanitization
- 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 section.)
- Complete Certificate of Data Sanitization
- Sanitization Status Code: DS

Portable USB Drives or Memory Cards - (Removable Media)

For all:
- Destroy disc using approved destruction methods (See Sanitization Requirements section.)
- Complete Certificate of Data Sanitization
- Sanitization Status Code: Removeable Media Destruction Successful (RMDS)

Data Storage Drive Devices – HDD and SSD via SCSI, IDE, ATA, SATA, eSATA, and NVMe (PCI Express)

For an operational drive:
- An approved OTS Overwrite standard operating procedure must be followed:
  - Data Sanitization Drive Single Pass Overwrite Procedure (See Single Pass section.)
  - Data Sanitization Drive Triple Pass Overwrite Procedure (See Triple Pass section.)
    NOTE: Triple Pass Overwrite is required for sanitization of CJIS or other Restricted data.

If an Agency or OTS resource prefers to utilize an alternate overwrite procedure or solution:
- The alternate procedure must be documented
- 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 Data Sanitization label
- Complete Certificate of Data Sanitization
- Sanitization Status Code: Overwrite Successful (OWS)

If approved overwrite procedure failed:
- Complete Certificate of Data Sanitization
- Sanitization Status Code: Overwrite Failure/Marked for Destruction (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
        - ❖ Complete Certificate of Data Sanitization
        - ❖ Sanitization Status Code: OWFD
        - ❖ Affix LPAA Data Sanitization label to the original (parent) device

- If SSD:
    - Destroy drive using approved destruction methods (See Sanitization Requirements section.)
    - Complete Certificate of Data Sanitization
    - Sanitization Status Code: OWFDS
    - Affix LPAA Data Sanitization label to the original (parent) device

NOTE: Electronic equipment that has been sanitized then stored, or destroyed, must be documented using the OTS Media Storage and Sanitization Log.

Backup Tapes - (Magnetic Tape)

For all:

- If degausser is available:
    - Degauss
    - Complete Certificate of Data Sanitization
    - Sanitization Status Code: (Degauss Successful) DGS

- If degausser is not available:
    - Destroy tape using approved destruction methods (See Sanitization Requirements section.)
    - Complete Certificate of Data Sanitization
    - 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

- Complete Certificate of Data Sanitization
- Sanitization Status Code: (Power Reset Successful) PRS

EAPROM, EEPROM, or EPROM - (ROM)

For all:

- Destroy media using approved destruction methods (See Sanitization Requirements section.)
- Complete Certificate of Data Sanitization
- Sanitization Status Code: DS

BIOS/UEFI Secure Wipe Feature on a Hard Drive

Enter your system BIOS/UEFI settings, navigate to the storage options, select the target drive, and look for a "Secure Erase" or "Data Wipe" option, then follow the prompts to initiate the secure erase process; exact steps may vary based on your computer manufacturer and BIOS version.

Key steps:

- Access BIOS/UEFI: Restart your computer and press the designated key (usually F2 or Del) to enter the BIOS/UEFI settings during boot.
- Locate storage settings: Within the BIOS menu, navigate to the section related to storage devices or hard drives.
- Select target drive: Choose the hard drive you want to securely erase.
- Find Secure Erase option: Look for a "Secure Erase" or "Data Wipe" option within the drive settings.
- Initiate wipe process: Select the Secure Erase option and follow any on-screen prompts to confirm the operation.
- Complete Certificate of Data Sanitization
- Sanitization Status Code: Overwrite Successful (OWS)
- Affix an LPAA Data Sanitization Label to the device

Check compatibility:
Not all hard drives or BIOS versions support the Secure Erase feature, so verify if your system is compatible before attempting.

NOTE: If the data overwrite single pass process cannot be performed for any reason, the hard drive will be required to be degaussed or appropriately destroyed. Refer back to the Approved Processes section of this document for additional guidance on degaussing and destruction.

Drive Overwrite Procedures

Single Pass Overwrite

This is the approved procedure to utilize when a workstation or laptop hard drive requires data sanitization.

Equipment Required:

- SATA \ IDE Drive Cradle (if drive has been extracted from the parent asset)
- Motherboard with M.2 connector or SATA to NVME M.2 adapter.
- OTS Laptop
- Louisiana Property Assistance Agency (LPAA) Data Sanitization Label
- Certificate of Data Sanitization
- Single Pass Data Overwrite Software with Manufacturer's instructions.

NOTE: Overwrite software must meet or exceed requirements set within NIST Special Publication 800-88, Rev. 1, Guidelines for Media Sanitization.

Procedure:

If drive has been extracted from the asset:

1. Connect OTS Laptop to SATA / IDE Drive Cradle.
   - Insert drive into SATA / IDE Drive Cradle
   - Go to step 2 (below).

If drive is still in a workstation:

1. Follow the software manufacturer's instructions for Single Pass data overwrite and verification.
   - If the drive does not show up in boot menu:
     - Extract the drive and reset process booting from another device.
     - If drives not show up a second time, extract drive (if needed) and mark for destruction.
     - Follow the Approved Process for degaussing or destruction as outlined in this document.
   - If overwrite fails with any error messages:
     - Extract the drive and mark for destruction.
     - Follow the Approved Process for degaussing or destruction as outlined in this document.
2. If the overwrite procedure completes successfully, the software used must display a successful message indicating the drive has been rendered unusable.
3. Place a Louisiana Property Assistance Agency (LPAA) Data Sanitization Label on the device.
4. Complete the Certificate of Data Sanitization.
5. Place the device in the area appropriate that is designated for successfully sanitized equipment.

NOTE: If the data overwrite single pass process cannot be performed for any reason, the hard drive will be required to be degaussed or appropriately destroyed. Refer back to the Approved Processes section of this document for additional guidance on degaussing and destruction.

Triple Pass Overwrite

This is the approved procedure to utilize when a workstation or laptop hard drive requires data sanitization.

Equipment Required:

- SATA \ IDE Drive Cradle (if drive has been extracted from the parent asset)
- Motherboard with M.2 connector or SATA to NVME M.2 adapter.
- OTS Laptop
- Louisiana Property Assistance Agency (LPAA) Data Sanitization Label
- Certificate of Data Sanitization
- Triple Pass Data Overwrite Software with Manufacturer's instructions

NOTE: Overwrite software must meet or exceed requirements set within NIST Special Publication 800-88, Rev. 1, Guidelines for Media Sanitization.

Procedure:

If drive has been extracted from the asset:

1. Connect OTS Laptop to SATA / IDE Drive Cradle.
   - Insert drive into SATA / IDE Drive Cradle
   - Go to step 2 (below).

If drive is still in a workstation:

1. Follow the software manufacturer's instructions for Triple Pass data overwrite and verification.
   - If the drive does not show up in boot menu:
     - Extract the drive and reset process booting from another device.
     - If drives do not show up a second time, extract drive (if needed) and mark for destruction.
     - Follow the Approved Processes section.
   - If overwrite fails with any error messages:
     - Extract the drive and mark for destruction.
     - Follow the Approved Processes section.
2. If the overwrite procedure completes successfully, the software used must display a successful message indicating the drive has been rendered unusable.
3. Place a Louisiana Property Assistance Agency (LPAA) Data Sanitization Label on the device.
4. Complete the Certificate of Data Sanitization.
5. Place the device in the area appropriate that is designated for successfully sanitized equipment.

NOTE: If the data overwrite triple pass process cannot be performed for any reason, the hard drive will be required to be degaussed or appropriately destroyed. Refer back to the Approved Processes section of this document for additional guidance on degaussing and destruction.

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

References

OTS Information Security Policy (ISP)
LPAA POL 201401
NIST SP 800-88 Rev. 1 - Guidelines for Media Sanitization

Definitions and Terms

The terms and definitions below are listed for the purpose of this document.

- Agency – organizational units within the Louisiana Division of Administration (DOA) established to provide services to the citizens of Louisiana.
- Certificate of Data Sanitization - LPAA's approved sanitization log format (i.e., Certificate of Destruction or Data Erasure Certificate).
- Clearing Method – this method involves overwriting data (either with a single pass or multiple passes), performing a factory reset, or simply removing power from the device. It ensures that no residual data remains even when advanced forensic tools attempt data recovery. This method ensures that no data can be recovered.
- Confidential or Restricted Data – Confidential Data is data that the unauthorized disclosure of could seriously and adversely impact an Agency, third party, suppliers, individuals, or the State of Louisiana. Additionally, Confidential Data has been specifically excluded or granted exemption within the State's Public Records Law. Restricted Data is data that requires strict adherence to legal obligations such as Federal, State, or local law, specific contractual agreements, or data specifically designated as Restricted Data in applicable state or Agency policy. The unauthorized disclosure of Restricted Data is expected to have a severe or catastrophic adverse effect on an Agency, partners, individuals, or the State of Louisiana. Additionally, Restricted Data has been specifically excluded or granted exemption within the State's Public Records Law.
- Data Sanitization – 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.
- Destruction Method – this method includes shredding (for printed material), pulverizing, melting, incinerating, or disintegrating the device. This method ensures that no data can be recovered.
- Incineration – incinerate at temperature greater than 650°C.
- LPAA Data Sanitization Label – must be affixed to every item approved for surplus before LPAA's staff will accept the item into its inventory. Label must include the word "Sanitized", technician's initials, date of sanitization, and be placed next to the state asset tag.
- Purging Method – this method is achieved through degaussing, which effectively neutralizes magnetic fields on storage media. It's essential to use approved and serviced equipment for this process. This method ensures that no data can be recovered.
- Risk Management – the process of identifying, controlling, and minimizing the impact of uncertain events on system resources.
- Sanitization Status Code – used to categorize sanitization actions taken on a storage device or media and indicate the level of protection against data recovery.
- Single Pass Sanitization – a method of data sanitization that involves overwriting data with a single pass of a fixed pattern or random characters.
- Triple Pass Sanitization – a method of data sanitization that involves overwriting data with three (3) individual passes of a fixed pattern or random characters.
- Third Party Sanitization – refers to the process of using an external service provider to perform data sanitization activities.

Acronyms

- BD - Blu-ray Disk
- BIOS – Basic Input Output System
- CJIS - Criminal Justice Information Systems
- DGS - Degauss Successful
- DRAM - Dynamic Random-Access Memory
- DS – Data Sanitization
- EEPROM – Electronically Erasable Programmable Read-Only Memory
- eSATA - External Serial Advanced Technology Attachment
- HDD - Hard Disk Drive
- IDE – Integrated Development Environment
- ISP – Information Security Policy
- LPAA – Louisiana Property Assistance Agency
- MFD - Multifunction Device
- MRFMD - Machine Reset Failure/Marked for Destruction
- MRS - Machine Reset Successful
- ND – No Drive
- NIST – National Institute of Standards and Technology
- NVMe – Non-Volatile Memory Express
- NVRAM - Non-volatile Random-Access Memory
- OMDS - Optical Media Destruction Successful
- OTS – Office of Technology Services
- OWFMD - Overwrite Failure/Marked for Destruction
- OWS - Overwrite Successful
- PRS - Power Reset Successful
- RD – Removed Drive
- RMDS - Removeable Media Destruction Successful
- SCSI – Small Computer System Interface
- SLA - Service-Level Agreement
- SRAM - Static Random-Access Memory
- SSD - Solid-State Drive
- UEFI - Unified Extensible Firmware Interface
- USB – Universal Serial Bus

Owner

Division of Administration, Office of Technology Services, Information Security

Contact Information:
OTS Information Security Team - InfoSecTeam@la.gov
OTS Information Security Compliance Team – InfoComp@la.gov
OTS User Support - OTSSupport@la.gov

Effective Date: 12/08/2014

Data Classification Level: **Public**

Revision History

Version	Date	Description	Author
1.00	10/21/2014	Creation.	Ivory Junius
1.01	12/08/2014	Content and format revision.	Dustin Glover
1.02	02/05/2015	First, status code added, drive removal for workstations. Second, removed verbiage causing potential confusion for operational printers that do not store data. Finally, document format changes/improvements.	Dustin Glover
1.03	04/04/2023	Reviewed and reformatted document with internal standard procedure layout.	Carla Simoneaud
1.03	10/15/2024	Replaced pictures with text, updated to current EUC and LPAA processes and verbiage, replaced references to specific programs/software with references to NIST SP 800-88 Rev. 1 requirements. Checked formatting, spelling, and grammar.	Marnie Cook
1.03	10/24/2024	Combining Policy and Procedures into one document.	Susan Eversull and Carla Simoneaud
1.03	10/28/2024	Review, update, and added BIOS/UEFI.	Donny Brown

Authorization:

DocuSigned by:
Derek Williams
8EDEB03D4FD14E7...

12/20/2024

Derek Williams, State Chief Information Officer — Date

DocuSigned by:
Chase Hymel
EC675CD5A9734DE...

12/23/2024

Chase Hymel, Chief Information Security Officer — Date

IMPORTANT NOTE: The Chief Information Security Officer oversees actions to create, monitor, and enforce Statewide Information Technology policies and procedures, and identify and address vulnerabilities and risks, and manage security incidents. Consequently, the policy and procedures are reviewed and updated by Information Security Compliance Team to ensure federal regulations and safeguards are met. Any user found to have violated Office of Technology Services Information Security policies and procedures may be subject to disciplinary action, up to and including dismissal, or criminal or civil legal actions.