TITLE: Data Destruction and Disposal

NUMBER: BUL-6916.1

ISSUER: Soheil Katal
Chief Information Officer
Information Technology Services

Joel Simangan
Chief Information Security Officer
Information Technology Services

DATE: July 26, 2024

ROUTING
All Employees
All Locations

PURPOSE: The purpose of this policy is to provide the authorized methods for securely and permanently destroying protected pupil and non-pupil District records.

MAJOR CHANGES: This revision replaces BUL-6916, dated August 28, 2017. It was revised to:

- Update the names of issuers.
- Focus on data destruction, including the handling of Cloud-Hosted data.
- Align with National Institute of Standards and Testing (NIST) SP 800-88 guidelines for media sanitization.
- A certificate of sanitization from third-parties is required for using or storing district data.

GUIDELINES:

SCOPE

The purpose of this policy is to provide the authorized methods for securely and permanently destroying District Protected and Non-Public information, as defined in Bulletin 1077.2 Information Protection Policy. This policy assumes the data disposal methods herein do not violate other applicable record retention policies, procedures, regulations, laws, or Board Rules (refer to Bulletin 6825.0 Records Retention and Destruction). Additionally, before data can be disposed of, it must not be:

- Subject to a legal hold or public records request.
- Relevant to a potential or active criminal, civil, or administrative case.
- Subject to an outstanding public or parental request to inspect or review.
- Required by third-parties to perform work on behalf of the District or other authorized educational function.

This policy applies to all District employees, volunteers, and contractors that store, secure, retrieve, publish, and destroy Protected and Non-Public Information, including Sensitive Security Information (SSI).

OBJECTIVES

1. Completely destroy Protected or Non-Public District Information located on obsolete or repurposed IT equipment before the equipment is recycled, disposed of, salvaged, refurbished, sold, or donated to external parties for the purpose of:
    a) Protecting Privacy
    b) Complying with federal regulations
    c) Protecting sensitive District business operations
    d) Complying with software licensing agreements
    e) Breach of software licensing agreements

2. To securely and effectively render Protected and Non-Public District Information on third-party cloud providers as unreadable and unrecoverable.

3. To reduce the cost of maintaining and supporting storage devices in District data centers by minimizing the amount of unnecessarily archived information or reduce third-party cloud-hosting costs by minimizing the amount of unnecessarily provisioned storage space.

4. To streamline District operations by reducing the time spent on unnecessary backups and discovery requests.

5. To align with the National Institute of Standards and Testing (NIST) SP 800-88 guidelines for media sanitization.

DEFINITIONS

Cloud-Hosted Data: Data stored, managed, and processed on a network of remote third-party servers versus local District servers or computers.

Cryptographic Erasure (CE): A method of sanitization in which the key used to encrypt the target data target is removed, making recovery of the decrypted target data infeasible.

Degaussing: A process that reverses the magnetizing field of a disk so that information cannot be physically tracked on the platters, making the drive permanently unusable.

Encryption: The process of transforming information using a cryptographic algorithm (called a cipher) to make it unreadable to anyone except those with special knowledge, usually called an encryption/decryption key.

Personally Identifiable Information (PII): Any information about an individual that can be used to distinguish or trace an individual's identity (e.g., name, social security number, date of birth, address, etc.)

Sensitive Security Information (SSI): Critical information that, if publicly released, could be useful to threat agents in exploiting security vulnerabilities. SSI is exempt from disclosure under the Freedom of Information Act and may include, but is not limited to, investigations, detailed floor plans, security incident plans, security training materials, network configuration files, and lists of critical technology infrastructure.

Self-Encrypting Drives (SED): A type of hard drive that automatically and continuously encrypts the data on the drive without any user interaction.

Sanitization: A process to render access to data on media infeasible. Clearing, purging, and destruction are techniques that can sanitize media.

DISPOSAL AND DESTRUCTION OF EQUIPMENT AND MEDIA

Whenever equipment or media is disposed of, any non-public or confidential data must be sanitized in compliance with NIST SP-800-88.

EQUIPMENT

This policy applies to all electronic and hard copy records containing Protected or Non-Public District information stored on, but not limited to:

- Self-Encrypting Drives
- Office Equipment, including printers, copiers, and cameras
- Network Devices
- Hard Copy Storage
- District-issued mobile phones
- Magnetic Storage Media
- Optical Media
- Flash Memory-Based Media
- Cloud-Hosted Data

Self-Encrypting Drives

Self-encrypting drives (SEDs) with integrated ‘always-on’ encryption significantly lower the chance of District information being left on devices. After data is encrypted, it can be destroyed by just destroying the media encryption key (MEK) used to encrypt the information initially. This process leaves encrypted text on the media that cannot be deciphered. District data custodians may use this method to sanitize large storage media quickly. However, it must not be used when the drive was encrypted after Protected or Non-Public District Information was stored on the device without being first sanitized.

Office Equipment
If supported, office equipment such as copiers, printers, cameras, fax machines, and document scanners must be configured by the equipment owner to remove queued, unprocessed files automatically and securely from their internal magnetic or flash-based storage media. Equipment owners must ensure that office equipment to be recycled, disposed of, salvaged, refurbished, or donated to external parties have their internal storage media sanitized using methods authorized herein and all network configuration information cleared by performing a full manufacturer's reset.

Network Devices
Sensitive security information (SSI) on network devices may be cleared rather than physically destroyed. Network administrators must perform a full manufacturer's reset to clear network devices, such as routers, switches, and access points, to their default factory settings to destroy SSI. Any removable storage media containing SSI used by network devices must be cleared through methods appropriate to the media type authorized herein.

Hard Copy Storage
Paper records with Protected and Non-Public Information must be destroyed using shredders that produce strips no wider than 6mm in length or particles no larger than 320 mm, or they must be pulverized/disintegrated using disintegrator devices. Microfilm or other reduced-image photo negatives must be destroyed by burning until the residue is reduced to white ash.

District-Issued Mobile Phones
Due to the diversity of mobile devices in District circulation, the methods for properly sanitizing Protected or Non-Public Information on them may vary. Cryptographic erasure is the easiest and preferred method for sanitizing mobile phones. However, if this option is not supported, a full reset to default factory settings must be performed to erase all content and settings.

Magnetic Storage Media
a) Floppy Disks: Information on floppy disks must be destroyed by degaussing, incineration, pulverization, or shredding.
b) Cassettes: All portions of the magnetic tape should be overwritten once with known non-sensitive signals.
c) Hard Drives: This group of storage media includes Serial Advanced Technology Attachment (SATA), Parallel Advanced Technology Attachment (PATA), External Serial Advanced Technology Attachment (eSATA), Small Computer System Interface (SCSI), and peripherally attached drives. Cryptographic erasure is the easiest and preferred method for sanitizing magnetic storage media. However, if this option is unavailable, these drives may be sanitized by executing vendor-

supported SANITIZE commands, degaussing, incineration, pulverization, or shredding.

Optical Media
Protected or sensitive security information on CDs, DVDs, and Blu-Ray discs must be sanitized by incineration or shredding.

Flash Memory-Based Storage Devices
a) Solid State Drive (SSD): Protected and Non-Public Information on SSDs can be sanitized using the same techniques as magnetic media, except for degaussing.
b) USB Removable Media and Memory Cards: Due to the diversity of USB media in general circulation, methods for properly sanitizing Protected or Non-Public Information may not be supported, or the interface to perform sanitization is not standardized, making it difficult to develop accurate procedures across the District. Protected or Non-Public Information must be sanitized by incineration, pulverization, or shredding. Memory cards include SD, SDHC, MMC, compact flash memory, micro-drives, and memory sticks, which may be sanitized using the same techniques as USB removable media.

Cloud-Hosted Data
Due to the nature of cloud hosts providing services for multiple tenants and separating data object(s) by physical and logical means, the District must only select cloud hosts that can ensure no “data remnants” exist when space previously used by the District is allocated for use to another party. This is to consider that cloud hosts can have multiple tenants storing data in the same physical storage medium and use digital data deletion techniques instead of physical destruction when a tenant deletes their data object(s).

Since the District does not have direct physical control of the data storage medium, secure data deletion for cloud hosts should be based on processing requests for data deletion and being capable of:
1. Logging the date, time, and authorized user making the request to delete the data object(s).
2. Disabling all new attempts to access the data object(s) by either/or:
    a) Using cryptographic erasure to render the data unreadable by deleting the encryption keys needed to decrypt the data.
    b) Removing the mapping from the name to the data object makes it inaccessible even to the owner.
    c) Zero-filling the object before returning the space for use and/or n-pass overwriting the object with random data.
3. Logging the date and time the deletion request is completed.
4. Making the log information accessible or exportable.

The District must also only select cloud-hosting providers capable of meeting relevant legal and regulatory requirements for the data they host regarding the destruction of physical media storage devices once a cloud host decides to decommission the physical media.

CERTIFICATE OF SANITIZATION

All employees responsible for inventory and management of equipment and media containing Protected or Non-Public Information must ensure that whenever equipment or media is disposed of, it must be sanitized in compliance with NIST SP-800-88. As stated in NIST 800-88 sanitization guidelines, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. Third-parties that are deposing of data on behalf of the District must also provide a certificate of sanitization.

Certificates of sanitization must be retained for five (5) years. Refer to **Attachment A** for an example of a Sanitization Form.

At a minimum, the certificates of sanitization must contain the following:

1. Information about the media
2. Date of erasure/destruction
3. Method of erasure/destruction
4. The person who carried out the process
5. Validation that the sanitization events were successful

Third-parties that use or store District data must provide a certificate of sanitization at the termination of their engagement.

Contact the ITS Help Desk at https://www.lausd.org/helpdesk for assistance in disposing of equipment and media.

VALIDITY AND DOCUMENT MANAGEMENT

The owner of this document is the Chief Information Security Officer (CISO), who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of incidents arising from failure to erase or destroy information in a manner specified in this document.
- Number of destroyed devices with sensitive security information for which no record is kept.

REVIEW AND UPDATES

This policy will be reviewed periodically to ensure its effectiveness and may be updated as needed.

RELATED RESOURCES:

- BUL-1077.2, Information Protection Policy
- BUL-6825.0, Records Retention and Destruction
- BUL-095100.2 Site Computer Inventory Policy
- Family Educational Rights and Privacy Act (FERPA), 34 CFR Part 99
- NIST Special Publication 800-88 Rev. 1, Guidelines for Media Sanitization

AUTHORITY: This is a policy of IT Security.

ATTACHMENTS: Attachment A - Media Sanitization and Data Destruction Certification Form

ASSISTANCE: For assistance or further information, please contact IT Security at information.security@lausd.net.

ATTACHMENT A

Media Sanitization and Data Destruction Certification Form

Person Performing Sanitization	
Name:	Employee Number:
Organization:	Location Code:
Media Information	
Type of Media: ☐ Magnetic ☐ Solid State ☐ Flash ☐ Optical ☐ Other: _____	
Manufacturer:	Model Number:
Serial Number:	Asset Tag:
Storage Capacity:	Destruction Date:
Backups Exist? ☐ Yes ☐ No	
Data Destruction Details	
Method Type: ☐ Clear ☐ Purge ☐ Media Damage ☐ Media Destruction	
Method Used: ☐ Degauss ☐ Overwrite ☐ Block Erase ☐ Crypto Erase ☐ Other _____	
Other Details:	
Tool Used (if applicable):	
Verification Method:	
Notes:	
Media End Destination	
☐ Internal Reuse ☐ External Reuse ☐ Recycling ☐ Return to Manufacturer ☐ Other _____	
Details:	
Signature	
I certify that this information is complete and accurate to the best of my knowledge.	
Signature:	
Date:	
Validation	
I certify that the erasure of the media as documented has been validated and confirmed.	
Name:	Employee Number:
Signature:	
Date:	