

To: All Health Care Services Division Property Managers

From: John Kelly, Asset Management

RE: DATA SANITATION PROCEDURE

In order for the Health Care Services Division (HCSD) to comply with State of Louisiana Office of Information Technology policy IT-Pol-003 (Data Sanitation) the following procedure will be followed by all Business Units of the Health Care Services Division.

Whenever magnetic storage devices, optical storage media and non-volatile memory devices are surplus, transferred to another government entity or are subject to destruction they must be sanitized. The Health Care Services Division has determined the appropriate method of sanitation is destruction. This method of sanitation is in compliance with Office of Information Technology policy IT-Pol-003 and Louisiana Property Assistance Agency (LPAA) guidelines.

It shall be HCSD's procedure after the hard drive is destroyed to label each surplus computer with a label which states "HARD DRIVE DESTROYED".

A copy of this procedure shall be forwarded to LPAA to conform to their notification requirements.

Health Care Services Division Agencies:

39000 – Health Care Services Division – Administration

39004 – Earl K. Long Medical Center

39006 – Huey P. Long Medical Center

39010 – University Medical Center of Louisiana

39012 – W.O. Moss Medical Center

39014 – Lallie Kemp Medical Center

39015 – L.J. Chabert Medical Center

39016 – Washington-St. Tammany Medical Center

15400 – Medical Center of Louisiana New Orleans



State of Louisiana
DIVISION OF ADMINISTRATION

LOUISIANA PROPERTY ASSISTANCE AGENCY

KATHLEEN BABINEAUX BLANCO
GOVERNOR

JERRY LUKE LEBLANC
COMMISSIONER OF ADMINISTRATION

To: All Property Managers

From: Floyd Rector, LPAA

RE: Data Sanitization

Pursuant to LAC 4:XV.101, et seq., the Office of Information Technology (OIT) has updated I.T. Policy in the following area:

Data Sanitization (IT-Pol-003)

All State agencies must comply with the attached I.T. Policy when magnetic storage devices, optical storage media, and non-volatile memory devices are surplus, transferred to another state agency, or scrapped/dismantled for parts if the data is determined by the owner to be security-sensitive. All agencies must establish policies and procedures to ensure compliance with this policy.

Each agency must notify Louisiana Property Assistance Agency of the method they intend to use for data sanitization. If you choose L. "Destroy," you must place a label on each surplus computer notifying "HARD DRIVE DESTROYED."

If you should have any questions regarding the I.T. Standards, please contact Mike Gusky at 225-219-9470.



KATHLEEN BABINEAUX BLANCO
GOVERNOR

State of Louisiana
**DIVISION OF ADMINISTRATION
OFFICE OF STATEWIDE TECHNOLOGY**

JERRY LUKE LEBLANC
COMMISSIONER OF ADMINISTRATION

1/25/2005

Office Of Information Technology

Information Technology Bulletin 04-12

Subject: I.T. Policy

Pursuant to LAC 4:XV.101, et seq., the Office of Information Technology (OIT) is updating I.T. Policy in the following area:

- Data Sanitization (IT-POL-003)

All entities under the authority of OIT as defined by R.S. 39:15.1, et seq, must comply with the above I.T. Policy.

If you have any questions regarding the published I.T.Standards, please contact Mike Gusky at 225-219-9470.

Office of Information Technology Policy

DATA SANITIZATION

Purpose:

To define the minimum requirements for the removal of security-sensitive data from agency computer storage media prior to being transferred to another government entity, or surplused. For the purpose of this policy, security-sensitive refers to data that is confidential or protected from disclosure by either federal or state laws.

Policy:

Magnetic storage devices, optical storage media and non-volatile memory devices that are surplused, transferred to another government entity or subject to destruction, must use a method of data sanitization compliant with the attached data sanitization matrix that was adapted from DoD specification 5220.22M if the data is determined by the owner to be security-sensitive.

Scope:

All entities under the authority of the Office of Information Technology, pursuant to the provisions of R.S. 39:15.1, et seq., must comply with this policy.

Responsibilities:

- Agencies must establish policies and procedures to ensure compliance with this policy.
- Agencies must adhere to the license terms and agreement for software on a computer that is being transferred to another agency or surplused.
- Agencies should conduct periodic checks to determine their method of sanitization is working correctly.
- Agencies must maintain records indicating the method of data sanitization utilized when personal computers are surplused or transferred to another agency.
- The owner of the data is responsible for determining if the data is security-sensitive.

Effective Date:

July 31, 2002

Reissued October 1, 2002 (revised policy format)

Reissued May 1, 2003 (revised scope statement)

Reissued January 12, 2005 (revised title, purpose, policy, scope, responsibilities)

Office of Information Technology Policy

**Office of Information Technology
Data Sanitization Matrix
Adapted from
DoD Specification 5220.22M**

Media	Procedure(s)
Magnetic Tape	
Type I*	a, b, or l
Type II**	b or l
Type III***	l
Magnetic Disk	
Floppies (e.g., 3.5inch, zip disks, etc.)	a, b, d, or l
Non-Removable Rigid Disk (e.g., hard drives)	a, b, d, or l
Removable Rigid Disk	a, b, d, or l
Optical Disk	
Read Many, Write Many (e.g., CD-RW)	l
Read Only	l
Write Once, Read Many (e.g., CD-R, CD+R, DVD+R)	l
Memory	
Dynamic Random Access Memory (DRAM)	c, f, or l
Electronically Alterable PROM (EAPROM)	i or l
Electronically Erasable PROM (EEPROM)	g or l
Erasable Programmable ROM (EPROM)	k, then c or l
Flash memory (FEPRM) (e.g., USB drives, xD Picture cards)	c, h or l
Programmable ROM (PROM)	l
Magnetic Bubble Memory	a, b, c, or l
Magnetic Core Memory	a, b, e, or l
Magnetic Plated Wire	c or l
Magnetic Resistive Memory	l
Nonvolatile RAM (NOVRAM)	c, f, or l
Read Only Memory (ROM)	l
Static Random Access Memory (SRAM)	c, f, or l
Sanitization Procedure Key	

- a. Degauss with a Type I degausser.

Office of Information Technology Policy

- b. Degauss with a Type II degausser.
- c. Overwrite all addressable locations with a single character.
- d. Overwrite all addressable locations with a character, its complement, then a random character and verify.
- e. Overwrite all addressable locations with a character, its complement, and then a random character.
- f. Remove all power to include battery power.
- g. Overwrite all locations with a random pattern, all locations with binary zeros, all locations with binary ones.
- h. Perform a full erase as per manufacturer's data sheets.
- i. Perform h. above, then c. above, three times.
- j. Perform an ultraviolet erase according to manufacturer's recommendation.
- k. Perform j above, but increase time by a factor of three.
- l. Destroy – disintegrate, incinerate, pulverize, shred, or melt.

This information was extracted in part from the US Department of Defense 5220.22-M Clearing and Sanitization Matrix.

*Type 1 magnetic tape includes all tapes with a coercivity factor (amount of electrical force required to reduce the recorded magnetic strength to zero) not exceeding 350 oersteds.

**Type 2 magnetic tape includes all tapes with a coercivity factor between 350 and 750 oersteds.

***Type 3 magnetic tape commonly referred to as high-energy tape (4 or 8mm tape are examples), includes all tapes with a coercivity factor between 750 and 1700.