State of Louisiana

Office of Technology Services

Data Sanitization Policy

Purpose

The Office of Technology Services (OTS) continues its commitment to the information security requirements for maintaining data privacy and protection. This policy clearly indicates the responsibilities and actions required to ensure data is properly removed prior to the release or disposal of equipment.

Scope

All entities under the authority of OTS, pursuant to the provisions of R.S. 39:15.1, et seq., shall comply with this policy.

This policy does not apply to any device or electronic media seized, confiscated, or requested as evidence to support any administrative, legal, or lawful action.

Definitions

(For the purposes of this document)

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

Device – any equipment, hardware, or system owned, managed, or utilized by an agency or its agents to transmit, store, or process data. Examples include, but not limited to: laptops, desktops, servers, routers, smart phones, PDAs, tablets, monitoring systems, printers, fax machines, or copiers.

Electronic Media – any media owned, managed, or utilized by an agency or its agents with the capability to store, transmit, or receive data. Examples include, but not limited to: CDs, DVDs, Hard Drives (HDD), Backup tapes, USB drives, SD cards, network attached storage, or internal system memory components (ROM and RAM).

Policy

Any electronic media or device subject to surplus, disposal, transfer, or otherwise permanently leaves the possession of a state agency or it's agents shall be sanitized using approved equipment, techniques, and procedures as required by the OTS Data Sanitization Requirements and Standards.

Responsibilities

Agencies shall:

- Review and ensure compliance with current data or record retention policies and directives prior to taking any approved actions to overwrite or destroy data.
- Establish operational processes to ensure compliance with this policy.
- Utilize the assigned data classification level, as required by OTS Data Classification Policy, to determine the required sanitization method.
- Maintain sanitization log records, as defined in OTS Data Sanitization Requirements and Standards, indefinitely.
- Report any violation of this policy directly to OTS Information Security resource in a timely manner.

Related Policies, Standards, Guidelines:
OTS Data Classification Policy
OTS Data Sanitization Requirements and Standards

Owner:
Division of Administration, Office of Technology Services

Effective Date:
11/15/2014

Revision History:

Date	Author	Description
2014-10-21	Ivory Junius	Creation
2014-11-02	Dustin Glover	Revision