Office of Information Technology
Policy

Data Sanitization

Policy:
Any items containing security sensitive data, including, but not limited to, magnetic storage devices, optical storage media and non-volatile memory devices, that are to be surplused, transferred, returned to another government entity, returned to the contractor or subject to destruction, must use a method of data sanitization compliant with the IT STD 1-17 Data Sanitization matrix. Some examples are computers (desktop, laptop, server), copiers, multi-function printers, external data storage/backup devices, PDAs, smartphones and network devices such as routers and firewalls.

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 and may use IT Bulletin 08-02 for guidance in data classification.

Related Policies, Standards, Guidelines:
IT STD 1-17 Data Sanitization
IT Bulletin 08-02 Data Classification Guideline

Owner:
OIT Security Office

Effective Date:
February 13, 2011