



STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 152 – Information Disposal and Media Sanitization Policy	POLICY NO: 09-10-NJOIT	
	SUPERSEDES: NEW	EFFECTIVE DATE: 04/08/2011
	VERSION: 2.0	LAST REVIEWED: 01/22/2015

ATTN: Directors of Administration and Agency IT Directors

1 PURPOSE

The purpose of the policy is to provide for the proper disposal or sanitization of media that have been damaged and/or are no longer needed. It is also written to ensure that the information contained on such media is completely expunged before it leaves the State of New Jersey’s control.

This policy applies to all media that a Department or Agency uses to store information. This policy is meant to establish a media disposal and sanitization process that is based on the classification of the information contained on the media. This policy is not intended to provide direction for records management, records retention, or records archiving, nor does it address the transfer of equipment within the State of New Jersey.

Agencies are reminded that the management and retention of all records stored electronically are subject to the retention and destruction-of-records rules of the Division of Revenue and Enterprise Services in the Department of the Treasury. When a law or other regulation requires records to be maintained longer, or if there is a litigation hold or a reasonable anticipation of litigation that would make the records needed for an inquiry or legal proceeding, then the extended time frame would take precedence.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey. [N.J.S.A. 52:18a-230 b](#). This policy defines New Jersey Office of Information Technology’s (NJOIT) role with regard to technology within the Executive Branch community of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.



3 SCOPE

This policy applies to all personnel including employees, temporary workers, volunteers, contractors, and those employed by contracting entities, and others who are tasked with the disposal or reallocation of the State of New Jersey property.

4 DEFINITIONS

Please refer to the Statewide Policy Glossary at <http://www.nj.gov/it/ps/glossary/>.

5 POLICY

All media will be properly disposed of and sanitized according to the [security classification](#) contained therein. All sanitization and disposal decisions are made based on the most stringent security classification of the information contained on the media regardless of the type of media. Before any media are sanitized or disposed of, information and system owners must ensure that the data owners are aware of and are a part of the approval process for the destruction of their data.

The NIST Guidelines for Media Sanitization are to be used as the standard for this policy. Any tools used for the disposal or sanitization of media must meet the standards in the [NIST Special Publication 800-88 Guidelines for Media Sanitization](#).

Departments and agencies shall ensure that business processes meet the NIST Guidelines for disposing or sanitizing of media. This NIST process must be implemented in such a manner as to ensure that all State media are properly sanitized of data and information before they leave the State of New Jersey's control. This includes any third-party involvement with said media for administrative, maintenance, or repair purposes.

State policy titled *Disposition of Excess & Surplus Computer Equipment*, Number [13-18-DPP](#) and procedure titled *Excess/Surplus Property Procedures*, Number [08-03-DPP](#) govern the disposal of all hardware declared excess and offered to other Departments/Agencies in coordination with the Surplus Property Unit, Division of Purchase & Property, and Department of the Treasury. These policies and procedures should be referred to as appropriate.

A record of all disposed hardware must be kept by all Departments and Agencies in accordance with the NIST Guidelines, as well as other State policies and regulations on equipment disposition.



6 EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date.

Failure to comply with this policy may result in disciplinary action. Requests for exceptions for non-compliance with this policy shall be processed in accordance with Statewide IT Circular [08-02-NJOIT, 111](#) – *Information Security Managing Exceptions*.