**NJ OFFICE OF INFORMATION TECHNOLOGY**
Chris Christie, Governor
E. Steven Emanuel, Chief Technology Officer

P.O. Box 212 www.nj.gov/it/ps/
300 Riverview Plaza
Trenton, NJ 08625-0212

# STATE OF NEW JERSEY IT CIRCULAR

**Title:** 1602 –Media Protection Policy

| | |
|---|---|
| **NO:** 14-07-NJOIT | **SUPERSEDES:** NA |
| **LAST REVIEWED:** January 7, 2014 | **DATE PUBLISHED:** January 7, 2014 |
| **VERSION:** 1.0 | **EFFECTIVE DATE:** Date of Signature |
| **FOR INFORMATION CONTACT**: Office of Policy and Planning | |

ATTN: Directors of Administration and Agency IT Directors

## I. PURPOSE

The policy's purpose is to protect the media that the State of New Jersey uses to store information that is sensitive and/or critical to operations. The policy addresses both confidentiality of data and the integrity of the media itself.

This policy applies to all media, whether paper or digital. This includes laptops and other portable computing devices, printouts, tapes, removable storage devices, and all other information storage media. This policy establishes protection based on the classification of the information contained on the media. It is not intended to provide direction for records management, records retention, or records archiving.

Agencies are reminded that the management and retention of all records stored electronically are subject to the retention schedules published by the Records Management Services unit of the Division of Revenue and Enterprise Services.

## II. 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.

## III. 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 protection of State of New Jersey information and property.

## IV. DEFINITIONS

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

## V. POLICY

Agencies shall establish physical and logical controls and procedures that protect system media (paper or digital), from unauthorized access during storage or transport or during events that lead to modification, destruction or loss. The extent of media controls shall be dependent upon factors including but not limited to: the type of data, the quantity of media, and the nature of the user environment.

Agencies will adhere to the following policies:

**A.** No confidential or personal State of New Jersey data shall reside on any mobile devices without documented agency authorization. Users must physically and logically safeguard the devices (both personally and state-owned) which host classified information used outside the office. All sensitive State information stored on mobile devices or storage devices is to be encrypted, in accordance to 12-02-NJOIT*, 132 – Portable Computing Use and Temporary Worksite Assignment Policy*

**B.** Both paper and digital media with a sensitivity classification of Secure or higher (Confidential and Personal) shall be stored in a secure location (such as lockable file cabinets or safes) when not in use, with access allowed only to authorized personnel. This classified media will be tracked by the Data Steward Organization.

**C.** The Data Steward Organization will mark or label all data with the appropriate sensitivity classification. Any media not labeled will be considered confidential by default.

**D.** Security controls shall be put in place to protect the confidentiality and integrity of data contained on removable storage media throughout the life of those storage media, including disposal. Access controls shall include physical protection of and accountability for removable media to minimize any risk to State of New Jersey data.

**E.** Only authorized personnel will transport of State of New Jersey paper and digital media, and the Data Steward Organization will track and secure media in locked containers if appropriate, based on the sensitivity of the information on the media.

**F.** When electronic media reaches the end of its lifespan, the electronic media will be properly disposed of and sanitized according to the security classification contained therein as described in 09-10-NJOIT*, 152 – Information Disposal and Media Sanitization*.

**G.** All printed media that contains data that is classified as State of New Jersey secure, confidential, or personal as described in *08-04-NJOIT, 130 Information Asset Classification Control Policy*, shall be shredded and destroyed to maintain the privacy, confidentiality, and integrity of the State of New Jersey's data.

Departments and Agencies must ensure that suitable business processes meet media protection guidelines set by the National Institute of Standards and Technology (NIST). State guardians must ensure that all State electronic and hard copy media are protected according to its classification while in the State of New Jersey's control. This includes any third-party involvement with said media for administrative, maintenance, or repair purposes.

## VI. EXCEPTIONS AND NON-COMPLIANCE

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

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*.

*Signature on File* *1/7/2014*

**E. STEVEN EMANUEL** **DATE**
**Chief Technology Officer-NJ Office of Information Technology**
**State Chief Information Officer**