NJ Office of Information Technology
Jon S. Corzine, Governor
Adel Ebeid, Chief Technology Officer

P.O. Box 212
300 River View
Trenton, NJ 08625-0212

www.nj.gov/it/ps/

State of New Jersey IT Circular

Title: 132 –Portable Computing and Removable Storage Devices Policy

NO: 09-18-NJOIT	**SUPERSEDES:**
DATE PUBLISHED: 12-21-2009	
VERSION: 12-21-2009	**EFFECTIVE DATE:** IMMEDIATELY
FOR INFORMATION CONTACT: Elizabeth Caldwell, Office of Policy and Planning (609) 633-0429	

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

The purpose of this policy is to ensure the confidentiality, integrity, and availability of the State of New Jersey information assets stored on portable computing or removable storage devices. Security controls are necessary to protect against theft of equipment, unauthorized disclosure of information, misuse of equipment, or unauthorized access to information assets.

II. AUTHORITY

This policy is established under the authority of the State of New Jersey P.L.2007.c.56. This order defines New Jersey Office of Information Technology's role with regard to technology within the community of the Executive Branch of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular to comply with changes in NJOIT or other agency policies.

III. SCOPE

This policy applies to all State personnel including employees, temporary workers, volunteers, contractors and those employed by contracted entities, and others who are authorized to access enterprise information resources.

IV. DEFINITIONS

A. Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

B. Integrity

Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

C. Availability

The assurance of timely and reliable access to and use of information. A loss of availability is the disruption of access to information or an information system.

D. Controls

A process of managing risk, including policies, procedure, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.

E. Information Assets

Information Assets are defined as all categories of electronic devices that process and/or contain digital information including but not limited to the following: databases, records, files, electronic documents, stored data, applications, and other software that is required to support business processes such as application software and system software.

F. Portable Computing Device

Portable or mobile computing refers to any device that allows a person to move from place to place while still being able to use information technology in a productive way.

G. Removable Storage Device

Any form of data storage which is not incorporated into the computer itself. In addition to providing a form of backup by removing data from a centralized computer system, removable storage allows people to easily carry data back and forth from a wide variety of devices and locations.

Portable computing and removable storage devices may include but are not limited to: palmtops, laptop computers, personal digital assistants (PDA's), universal serial bus (USB) port devices, compact discs (CD's), digital versatile discs (DVD's) flash drives, modems, mobile phones, and any other existing or future mobile or portable storage device that may connect to, access and/or store information or data.

V. POLICY

Each Department and Agency must establish controls to protect portable and removable computing devices, as well as protect and manage any sensitive information stored on them. To properly manage portable computing or removable storage devices, Departments and Agencies must establish a formalized methodology for maintaining an accurate and up-to-date inventory of all devices it owns and assigns. It is essential as part of this methodology to establish criteria for the usage and assignment of portable devices along with, what information is acceptable for storage on various types of devices. This will ensure each agency is prepared to quickly respond to and recover from security compromises as a result of loss or misuse of device.

Each Department and Agency will adopt and implement a policy and associated procedures crafted to fit the specific operational needs of that agency which at a minimum:

- Maintains an accurate account of who has been assigned devices.
- Identifies types of approved devices, as well as determines the permissibility of the use of personally-owned devices.
- Identifies methods for tracking or disabling devices as needed, based upon the classification of information assets stored on the devices.
- Establishes procedures for reporting and responding to loss or theft of devices.
- Identifies what information assets may or may not be stored on portable computing or removable storage devices.
- Determines approved methods for securing that information, as needed, appropriate to the information's classification. Security mechanisms could include encryption and endpoint data protection tools, tamper evident packaging, storage in secure areas.
- Determines appropriate methods for registering removal of portable devices from premises to an off-site location. No equipment, information or software should be taken off site without prior authorization.

- Ensures this information is communicated and enforced for all State employees, temporary workers, volunteers, contractors and those employed by contracted entities.

Each Department and Agency may, based upon its individual business needs or legal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security objectives defined in this document.

VI. EXCEPTIONS AND NON-COMPLIANCE

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 Enterprise Policy 08-02-NJOIT (111 – Information Security Managing Exceptions.

Signature on File *12/29/2009*

ADEL EBEID **DATE**
Chief Technology Officer