NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Odysseus Marcopolus, Chief Operating Officer
P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212
www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 132 - Portable Computing Use and Temporary Worksite Assignment Policy	**POLICY NO:** 12-02-NJOIT	
	SUPERSEDES: 98-15-OMB	**EFFECTIVE DATE:** 03/28/2012
	VERSION: 2.0	**LAST REVIEWED:** 05/03/2013

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The intent of this policy is to ensure the confidentiality, integrity and availability of State of New Jersey information assets stored on portable computing devices, as well as on state-owned removable storage devices and temporary worksite computer and/or peripheral equipment. It is designed to protect against theft, unauthorized disclosure of information, unacceptable use and unauthorized access. It also addresses prevention of the introduction of malware on portable computing devices, state-owned removable storage devices and temporary worksite computer and/or peripheral equipment. The policy specifies that a signed User Agreement must be obtained from employees desiring to access State computing resources using State-owned or personal portable computing devices.

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 (OIT) role with regard to technology within the Executive Branch community of State Government.

OIT 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 contracted entities, and others authorized to access enterprise information resources.

4 DEFINITIONS

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

Portable computing devices may include but are not limited to tablets, 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.

5 POLICY

OIT will serve as the central authority to ensure that a consistent and effective process is in place for a coordinated approach to protecting portable computing devices, temporary worksite computers and/or peripheral equipment.

To manage these devices and computer and/or peripheral equipment, departments and agencies must work jointly with OIT to establish a formalized methodology for maintaining an accurate and up-to-date inventory of all devices and computer and/or peripheral equipment that the State owns and assigns. An essential part of this methodology is to establish criteria for the usage and assignment of state-owned devices, temporary worksite computers, and/or peripheral equipment. The criteria must include the identification of what information is acceptable for storage on portable devices or temporary worksite computers. This will ensure that each department or agency is prepared to respond quickly to and recover from security threats and compromises as a result of loss or misuse of devices or computer equipment.

- Departments and agencies must meet the minimum security requirements, or exceed the security requirements based upon individual business needs or legal requirements put forth in this policy. If an agency or department desires an exception, refer to exceptions and non-compliance in section VII of this policy.

- Departments and agencies are required to follow Statewide *Policy 09-10-NJOIT, 152 – Information Disposal and Media Sanitization*.

- Personally identifiable or confidental data cannot be stored on any removable or onboard storage device or portable computing devices unless the storage is encrypted and can be accessed only with proper authentication of identity. Personally identifiable information is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any

other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Any employee assigned custody of any State–owned device, computer, and/or peripheral equipment shall be held accountable for such items. Accountability shall be extended to bearing the burden of reimbursing the State for items that cannot be accounted for, unless a loss or theft can be substantiated. Additionally, if an employee causes damage to any State-owned device, computer and/or peripheral equipment through carelessness or negligence, reimbursement for the repairs and/or replacement of the property may be the responsibility of the employee.

Under no circumstance may a State-owned device, computer, peripheral equipment, intellectual property or any inappropriate data defined in the State's policies be temporarily assigned to an employee's residence merely for the employee's convenience, nor shall the equipment be utilized for personal business.

5.1 Portable Computing Devices

5.1.1 Employees are only permitted to use State-owned removable storage devices.

5.1.2 Employees are not permitted to store any personally identifiable or confidential information on the device, or on removable storage, unless the information is encrypted and accessible only after identification has been authenticated.

5.1.3 Employees are permitted – temporarily for work purposes – to store a picture deemed personally identifiable or confidential on an encrypted device, but are required to process and remove the picture as quickly as it can be transferred to a secure system.

5.1.4 All authorized portable computing devices will be inventoried and managed by the State's Mobile Management System (MMS). The MMS will manage the portable computing devices to ensure proper security control protocols are installed and operating correctly.

5.1.5 Use of employees' personal portable computing devices is permitted under strict security controls. Users must sign an agreement with the State. Authorized devices will be inventoried and managed under the same security controls used for State-owned devices.

5.1.6 For both personal devices used for State purposes and State-owned portable computing devices and removable storage devices, regardless of their physical location, employees are subject to and must comply with all advisories, State directives not to delete data and information, litigation holds as directed by the State, and all relevant policies protecting data and information.

5.1.7 Departments, agencies or OIT retain the right to wipe or remove any State intellectual property from any portable computing devices, state-owned removable storage devices or computer equipment.

5.1.8 Departments, agencies, and OIT retain the right to remove and deny access for any portable computing and/or removable storage devices from any State system or network.

5.1.9 Departments and agencies must collect and retain signed User Agreements for each State-owned personal portable computing device that is provisioned by their IT unit to access State computer resources.

5.2 Temporary Worksite Assignment of State-Owned Computer and/or Peripheral Equipment

5.2.1 Departments and/or agencies may temporarily assign desktop computers, laptops, notebooks, and/or peripheral equipment for use at an employee's residence or for use on assignments at temporary work sites.

5.2.2 Temporary assignments of State-owned computers and/or peripheral equipment for use at employee residences shall be approved by agency management.

5.2.3 A department or agency's Property Removal Form shall be completed when state-owned computer and/or peripheral equipment is removed from the premises of a department or agency. The information contained on the document shall include, but is not limited to, the following:

5.2.3.1 The name of the employee taking custody of the equipment;

5.2.3.2 A description of equipment being removed, including model number and serial number;

5.2.3.3 The intended location (destination) of equipment; and

5.2.3.4 The authorized approval signature(s).

6 RESPONSIBILITIES

6.1 Departments and Agencies

6.1.1 Departments and agencies will work with OIT in establishing statewide standards and procedures to address the operational needs of all departments and agencies.

6.1.2 Departments and agencies must determine whether the use of a state-owned computer and/or peripheral equipment would be more effective in the off-premise location, and if the justification satisfies the criteria for authorizing the use, assignment and relocation of a State-owned computer and peripheral equipment via the agency's Property Removal Form.

6.1.3 Departments, agencies and OIT are responsible for enforcing the use of appropriate security software and compliance with policies regarding the use of the device, computer and/or peripheral equipment. Periodic security audits and reviews shall be conducted.

6.1.4 Departments and agencies must collect and maintain an accurate account register to track the distribution and retrieval of State-owned devices, computer, and/or peripheral equipment. Departments and agencies are required to collect and maintain an employee's portable computing user agreement, and, when necessary, have employees re-sign the portable computing user agreement when they are issued new portable computing devices or when this policy and/or the user agreement have changed.

6.1.5 Departments and agencies must determine the appropriate methods for registering the removal of the devices, computers and/or peripheral equipment from State premises to a temporary worksite. No equipment, information, or software should be taken off site without prior authorization.

6.1.6 Departments and agencies must develop procedures for the return of state-owned devices, computers and/or peripheral equipment when the user's employment or contract terminates, or the user's assignment no longer requires the maintenance of a State-owned device, computer, and/or peripheral equipment. The procedures shall address whether non-state data and software are permitted on the State-owned device, and if so, who is responsible for the removal of the non-State data and software when the device is returned.

6.1.7 Departments and agencies must annually review the list of employees with temporary worksite assignment of computers and peripheral equipment. Employees who no longer need equipment off-site should be required to return it immediately.

6.1.8 Departments and agencies shall require their Help Desks to record reports of device, computer, and peripheral equipment problems and seek direction on how to remedy these problems prior to initiating any service call.

6.1.9 Departments and agencies must maintain a centralized location for encryption key management.

6.1.10 Departments and agencies must collect and retain signed User Agreements for each personal portable computing device that is provisioned by their IT unit to access State computer resources.

6.2 NJ Office of Information Technology (OIT)

6.2.1 OIT is responsible for the oversight of this policy, including any related standards and procedures.

6.3 Employees

6.3.1 Employees must comply with this policy, and all State policies, standards, and guidelines referenced within this policy. In addition, authorized users shall comply with all applicable government codes of ethics and the New Jersey Conflicts of Interest Law, http://www.state.nj.us/ethics /statutes/conflicts/.

6.3.2 Authorized users will ensure that the security and patch management software on State-owned or personal portable computing devices and computers is installed, running, up-to-date, and active. Authorized users must not uninstall or disable any security software installed by the State.

6.3.3 It is the responsibility of authorized users to exercise reasonable caution to ensure that their State-issued equipment is kept secure from unauthorized access.

6.3.4 User Identification (User IDs) and passwords are the confidential information of the State, and therefore, no User IDs or passwords are to be shared.

6.3.5 Authorized employees must report the loss or theft of devices, computer, and/or peripheral equipment to their Department or Agency IT unit. A loss or theft must be reported within one hour after it is discovered.

6.3.6 Authorized employees should not store sensitive or confidential content on portable computing devices, unless this content is encrypted and software and/or hardware permits access only to users who can authenticate their identities.

6.3.7 Authorized employees must request proper authorization to remove State-owned computers and peripheral equipment from State facilities.

6.3.8 Authorized employees must complete their agency's Property Removal Form and obtain the valid signatures of authorization.

6.3.9 Authorized employees must show a completed Property Removal Form at the request of Security when entering or exiting the premise with state-owned computers and/or peripheral equipment.

6.3.10 Prior to leaving State service, the authorized employee is responsible for notifying the Human Resources Office and making the necessary arrangements for the return with proof of all state-owned computers and/or peripheral equipment to State control.

6.3.11 Authorized employees must take the necessary precautions to ensure the safety of the state-owned computer and peripheral equipment assigned to their care.

6.3.12 Authorized employees must contact the Help Desk within their department or agency to report problems, and they must seek direction on remedies prior to initiating any servicing of the computer and/or peripheral equipment.

6.3.13 Any unauthorized service performed at the initiation of the employee will be at the personal responsibility and cost to the employee.

6.3.14 Authorized employees must comply with all policies protecting State data or information. In addition, employees must follow State advisories and directions not to delete or destroy State data or information as well as honor litigation holds issued by the State.

6.3.15 Authorized employees must execute a User Agreement prior to gaining access to State computer resources through a personal portable computing device.

7 EXCEPTIONS AND NON-COMPLIANCE

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

A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. Exceptions and noncompliance with this policy shall be managed in accordance with Policy 08-02-NJOIT, *(111 – Information Security Managing Exceptions).*