The State of New Jersey's
PORTABLE COMPUTING USER AGREEMENT

I. PURPOSE

This Portable Computing User Agreement sets the responsibilities, security requirements, procedures, and policies for the use of the State's information system resources and services while connected to the State of New Jersey's Garden State Network or information systems through either a state-owned or a state-provisioned portable computing device. By entering into this Agreement, the authorized user agrees to abide by the New Jersey State Government Portable Computing Use policies, standards, and procedures.

Through this Portable Computing User Agreement, departments, agencies or New Jersey's Office of Information Technology (NJOIT) retain the right to immobilize, wipe, or remove any State data, information, or intellectual property from any portable computing device provisioned with State applications. The State is not responsible for the loss of personal information from a personal device provided by the State or used for State business. State applications and data will be erased immediately from stolen or lost devices.

II. GENERAL USE AND OWNERSHIP

A. Department, Agency, and NJOIT:

1. Departments, agencies, and/or NJOIT have the right to install monitoring and remote wiping software on devices connected to the State's Garden State Network or information systems. This software can be used at any time to monitor, manage and control State-owned applications.
2. Departments, agencies, and/or NJOIT retain the right to randomly audit devices connected to the State's Garden State Network or information systems to ensure State data or information security and to ensure that security software is up to date.
3. Departments, agencies, and/or NJOIT require that all portable computing devices used to connect to the State's Garden State Network or information systems:

   a. Enable password protection.

   b. Enable screen locking and screen timeout functions.

   c. Enable encryption for onboard storage or removable storage.

   d. Enable the control to wipe remotely and disabled the device if the device is stolen or lost.

   e. Enable management control or limit what applications are able to be downloaded and installed.

f. Install and enable anti-virus/anti-malware software.

B. It is the duty of the (*Department/Agency Employee*) to:

1. Accept responsibility for protecting, to the best of her/his ability, any and all State data or information stored on the portable device.
2. Not to store any personal identifiable or confidential information on the device.
3. Process and remove immediately any stored picture deemed personal identifiable or confidential from the device.
4. Not to store any IRS or Social Security Administration (SSA) provided data on any device.
5. Immediately report the loss or theft of a portable device covered under this agreement.
6. Protect the device from any deliberate attempt to circumvent the security measures put in place by the State.
7. Ensure that the device is password-protected.
8. Ensure the device has encryption capability to protect stored data, is protected with strong passwords, is enabled for inactivity timeouts, and locks out all possible users after several failed attempts to log in.

III. Authorized User

As an authorized user of the State's Garden State Network, I understand that the confidentiality and the protection of the State's data or information are of the highest importance. I have read and understand the State's Policy entitled Portable Computing Use and Temporary Worksite Assignment Policy, 12-02-NJOIT.

If my authorization is given by signing this Agreement, I understand that I must notify the Department or Agency IT unit within one (1) hour in the event that my State-owned or State-provisioned portable computing device is lost or stolen. I am aware that in the event of loss or theft, the device can be remotely wiped of all sensitive State data and capability, or of any other data or capability deemed necessary to protect State interests.

I agree not to dispose of my State-provisioned portable computing device, return it to my service provider, or give it to another individual without ensuring that my Department or Agency's IT unit has had a chance to secure any sensitive State data or information.

I understand that all State data, application or information received and stored on my authorized device is the property of the State and is to be used for State business only. I further understand that authorized personnel have the authority to monitor and control the use of my State-owned or State-provisioned portable computing device for usage, tracking and management purposes.

For the term of this Agreement, I acknowledge and agree that I will fully comply with all policies protecting State data or information, with advisories and directives not to delete or destroy State data or information, and with any litigation holds issued by the State.

I acknowledge and understand that the State will provision my device to permit access by installing software on my portable computing device that includes capabilities that could be used by my Department, Agency, and/or NJOIT to protect the physical security of my device and the integrity of State data or information. These functions include remote access control, GPS tracking and other security functions.

I agree to have State monitoring software installed on the device until otherwise directed by my Department, Agency, and/or NJOIT.

I acknowledge that I am aware that any violation of the statewide policy, standard, or procedure for Portable Computing may subject me to disciplinary action and/or lost of authorized access, which could even result in civil liability, criminal liability, or both.

Non-State owned devices which meet the above security criteria may be provisioned and used if the device owner acknowledges, and signs this agreement, which stipulates that their personal data on the device may be wiped out remotely if it is lost or stolen.

With my signature, I hereby acknowledge and I will abide by all the above stated responsibilities, policies, standards, and procedures.

____ ________________________
Signature Date

____
Print Name