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 portable computing device or a privately owned portable computing device (hereafter referred to as a personal device) that authorized personnel have provisioned with State applications. By entering into this Agreement, the authorized user agrees to abide by New Jersey State Government's Portable Computing Use policies, standards, and procedures regardless of whether they are using a state-issued device or a privately owned personal device configured for use in conducting State business.

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 loss of personal information from a portable-computing device provided by the State or from a privately owned personal device that has been configured for use with State networks. State applications and data will be erased immediately when devices are reported stolen or lost. Erasure of State applications will occur whether a device is State-issued or privately owned.

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 that are configured to allow connection to the State's Garden State Network or information systems. This includes any State-issued device and any privately owned personal device that authorized personnel have configured with State applications. 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 that are configured to connect to the State's Garden State Network or information systems. These audits are designed to protect the security of State data and information, 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 should data storage be authorized for State-business needs.

   d) Enable the control to wipe remotely and disable the device if it is stolen or lost. State data and applications will be wiped in the case of theft or loss, regardless of whether a device is provided by the state or is a privately owned personal device. The State also will erase private data if authorized by the owner of a lost or stolen personal device configured for connection to State networks and systems.

   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. Only data authorized by the State for storage on personal devices is allowed for usage in State applications. This authorized data should, whenever possible, remain in State applications, whether the device is state-issued or is a privately owned personal device configured for State usage.

2. Not store on any portable device any data collected by the State that meets the federally accepted definitions of Personally Identifiable Information (PII). This includes confidential data collected by the State such as Social Security numbers, tax information, and photographs that are used or can be used for identification purposes. It also includes confidential data the State has collected about employees, taxpayers, clients and customers, or anyone who is under State scrutiny, investigation, assistance or care. For a more complete definition of PII, see the glossary at http://nj.gov/it/ps/glossary/.

3. Not store any IRS or Social Security Administration (SSA) provided data on any device.

4. Immediately report the loss or theft of a portable device covered under this agreement, whether it be a State-issued device or privately owned, personal device configured for connection to State networks and systems.

5. Protect the device from any deliberate attempt to circumvent the security measures put in place by the State.

6. Ensure that the device is password-protected. In addition, the device should time out and require re-entering of a password after a reasonable period of inactivity by the user. All users should be locked out after several failed attempts to log in.

7. Ensure the device has encryption capability if needed to protect State data. Only data authorized for storage on portable computing devices should be stored in State applications. State data should remain within State applications. Contact your system administrator with any questions about what data, if any, can be stored on portable devices and how that data should be handled. Encrypted data should be safeguarded with its own strong passwords. Applications managing encrypted data should time out and require re-entry of passwords after periods of inactivity.

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 of the theft or loss of my State-owned portable computing device or my privately owned (personal) portable computing device that authorized personnel have provisioned with State applications. 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 if 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 – for usage, tracking and management purposes – authorized personnel have the authority to monitor and control the use of my State-issued portable computing device or of State provisioned applications in my privately owned, personal portable computing device.

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 also comply 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 a statewide policy, standard, or procedure for Portable Computing may subject me to disciplinary action and/or loss of authorized access, and could 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 _____