PERSONALLY OWNED DEVICE POLICY

Purpose: The purpose of this document is to establish the statewide policy for the use of personally owned devices by authorized users on state owned and operated networks. This policy serves to protect state networks, applications and data.

Policy: Personally owned devices include, but are not limited to, desktops, laptops, printers, personal digital assistants (PDAs), smart phones, tablets and storage devices such as flash memory (memory sticks), flash cards, portable hard drives, MP3 players and other peripherals that may connect to a PC or laptop.

As the use of smartphones and tablets grow in popularity, the demand to use these devices in the workplace has significantly increased. This use, referred to as Bring Your Own Device (BYOD), provides mobile productivity advantages and increases user satisfaction. Several platforms have been implemented to support the use of BYOD devices in participating agencies while minimizing risk. These include:

1. A mobile device management platform to allow secure access to state email by creation of a secure container to separate business and personal data.
2. A guest wireless network that provides Internet access while at the same time prohibiting access to the State’s data resources

The use of all personally owned devices must be approved by execution of the referenced Mobile Device User Agreement. The Department of Information Technology (DoIT) will neither install nor provide support for any personal devices connected to state networks, with the exception of the creation of applicable accounts. Approved BYOD devices are still treated as personal devices and are not considered ‘managed’ with DoIT support.

The use of any personally owned device accessing state owned equipment/networks not specifically approved is prohibited unless authorized as noted above.

This policy applies to authorized users connecting to state networks in any manner; via a state-owned computer at their normal workspace or remotely via an Internet-provided Virtual Private Network (VPN) or dial-in. Access to state resources via a state-owned smartphone device must use secure VPN access. Devices should not be setup as MiFi (My Wi-Fi) hotspots which provide access by additional devices.

Accountability: All authorized users of any state and/or agency network shall adhere to this policy.

It is the responsibility of all agency heads or their designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

Description: This policy serves to protect state networks from viruses and other potential security intrusions in addition to ensuring the security of confidential state data.

Reference: IT Standards Exception Policy
Mobile Device User Agreement
Mobile Device Security Policy