

# 9400-P175: Mobile Computing and Telework

## I. PURPOSE

This policy establishes requirements for the use of mobile computing devices and telework by anyone authorized to work on or access State Information Technology (IT) resources. This policy supplements Chapter 18, Section 1 of the State Personnel Rules, Telework.

## II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as “agencies”) and all entities covered in or under Policy 9200-P121: Third Party Security.

## III. POLICY

- A. All authorized users who remotely access State non-public IT resources shall, as a condition of access, ensure that the devices they use to connect to any State network are protected from malicious code per Policy 3200-P161: Malicious Code Prevention and that patches for their operating system and applications are installed per Policy 9400-P183: Technical Vulnerability Management.
- B. All devices authorized to connect to any State network and access State IT resources via the Internet shall do so via the appropriate encrypted connection, such as virtual private network (VPN) or secure sockets layer (SSL).
- C. Agencies shall verify to the greatest extent possible that anti-virus software and operating system security patches are up to date prior to or during the remote access connection. Devices that are a threat to the State network shall be disconnected and denied future access until their compliance is verified.
- D. State employees shall conduct electronic State business on State-owned computer resources. The use of non-state resources to conduct State business shall be specifically authorized by the Data Steward on a case-by-case basis after conducting a risk analysis. Group exceptions are not permitted.

Personnel granted exception to use non-state owned computer resources for State business shall be aware of the additional protection, dissemination, retention, and/or destruction responsibilities that come with having public records or restricted information on their personal computers or mobile devices.

- E. Encryption. Sending, storing or receiving restricted information on mobile devices shall be minimized to the extent possible. It shall be limited to business crucial functions only. If restricted information is sent, received or stored on mobile devices, it shall be encrypted and the encryption key escrowed with a designated agency designee. The type of encryption that is authorized to be used on mobile

## **9400-P175: Mobile Computing and Telework**

devices is stipulated by agency policy and standards until an enterprise encryption policy is written and approved.

- F. State liability for non-state IT resources. In all cases, the State is not responsible for the configuration, repair, replacement, or maintenance of non-state IT resources used for State business.
- G. Backups. Data on mobile computing devices shall be backed up to ensure that if the mobile device is lost, stolen, or inoperative, the data is still recoverable in accordance with Policy 8300-P162: Backup, Storage, and Restoration.
- H. Protection of mobile computing devices. Users of laptops and other mobile computing devices shall take all necessary precautions to protect against loss or theft. Users shall report missing or stolen devices through their immediate supervisor and the designated IT staff as soon as possible. If the missing or stolen property is known to contain restricted information, the requirement to report shall be immediate.

**CIO Approved Date: 1/28/2011**