

## MOBILE DEVICE USER POLICY

**Purpose:** The purpose of this policy is to ensure the consistent and secure use of State owned mobile devices managed by the Department of Information Technology (DoIT). Mobile devices governed by this policy include smartphones and tablet PCs.

**Policy:** A smartphone is a cellular phone that offers computing and connectivity ability. Smartphones are capable of connecting to and browsing the Internet and/or connecting to the State's enterprise email system. Examples include various Blackberry device models, the Apple iPhone, as well as a variety of smartphones which run the Windows Mobile and Android operating systems. Standard cellular phones are not capable of these advanced functions and are not covered under this policy.

Tablet PCs are flat, ultra-portable computers with a simple user interface operated primarily by a touch screen. Although not as powerful as a laptop or desktop computer, they provide full function browsing capability, run numerous business productivity applications and provide multimedia capability. Tablet PCs optionally provide a cellular and/or wireless connection to the Internet.

Mobile devices provide functionality and portability, but also introduce a security risk to the State's information assets. While these devices offer designs that enhance the user experience, they may not meet the state security requirements. Therefore, agencies must weigh the use of these systems against specific business requirements and the statewide Mobile Device Security Policy and standards.

Mobile devices are provided "FOR OFFICIAL USE ONLY," must have Agency Head or designee approval, and must comply with all standards established by DoIT. The distribution and use of these devices is not intended to replace or circumvent the telephone system or authorized access to state network resources. Individuals assigned a mobile device must comply with all applicable policies, procedures and standards, and must have a signed Mobile Device User Agreement on file.

### *Issuance, Purchase & Inventory*

All mobile devices must meet current DoIT standards or be reviewed and approved through the DoIT procurement process. The state standard Mobile Device Management (MDM) solution must be procured and installed on all state and personally owned mobile devices connecting to state resources.

The issuance of a smartphone or Tablet PC device shall be based upon assignment and operational necessity, at the discretion of the respective Agency Head. Each state agency is responsible for determining an employee's need for a smartphone or Tablet PC, and are responsible for billing, plan selection, or returns based on defective hardware or software. DoIT should be consulted prior to all purchase request submissions to ensure compliance to standardization requirements.

Each agency is responsible for inventorying all mobile devices, ensuring that user agreements are in place and that mobile devices are returned when no longer required or at the time of employee resignation and/or termination. All managed devices are subject to a periodic review by DoIT.

All personnel issued smartphones shall have a unique phone number that is associated with that person. If a spare smartphone is issued to personnel on a temporary basis, a log shall be maintained which includes the following: date of issue, the person's name, the cell phone

## **MOBILE DEVICE USER POLICY**

number, the make and model and serial number of the phone or tablet PC, and the anticipated return date.

### *Setup*

DoIT will provide initial setup according to established procedure and security policies. In this way, the State can ensure that its policies regarding personal and State-owned information are implemented, thereby improving information management and security.

Mobile devices will include standard applications that have been approved for use on state-owned devices. Although there are thousands of software options ranging from productivity tools to games, only the standard applications will be supported by DoIT.

Requests for installation of unsupported add-on software should be handled following the same procedure as for personal and laptop computer unsupported software requests, as documented in the IT Standard Operating Procedures. The installation of any additional application requires the authorization from the Agency Head or Designee prior to installation.

### *Support*

DoIT will provide basic instruction on the proper operation and will provide synchronization support for standard mobile devices assigned to authorized users. Due to the variety of mobile devices, support from DoIT will be provided on a 'best effort' basis. Free training is also provided by all State approved vendors and can be arranged through the agencies business office..

All e-mail or calendar synchronization issues will be handled through the Central Help Desk, [helpdesk@nh.gov](mailto:helpdesk@nh.gov), 271-7555 as priority 5 requests. The Help Desk Manager will have priority escalation approval authority so exceptions can be requested and considered on a case-by-case basis. If deemed appropriate, users may be requested to contact a vendor for further support. For example, a private toll-free number for Verizon Wireless support will be provided to employees assigned Verizon-supported mobile devices.

The use of non-standard and/or personally owned devices is prohibited without agency authorization and approved exception.

The Chief Information Officer (CIO) must approve exceptions to this policy prior to device procurement and activation.

**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 specifies the procurement, setup, and support for state-owned mobile devices.

**Reference:** Mobile Device User Agreement  
Mobile Device Security Policy  
Wireless Communications Policy  
Remote Access Policy  
IT Standards Exception Policy