



Department of Information Technology
Enterprise Policy

TITLE: *Mobile Device Security and Usage*

POLICY NUMBER: *DoIT-361-4001-A Version 1.0*

POLICY OWNER: *DoIT Deputy Secretary Miller*

POLICY SPONSOR: *DoIT Secretary Ackley*

AGENCY: 361

ISSUE DATE: *9/2/2014*

EFFECTIVE DATE: *9/2/2014*

REVISED DATE: *original*

NEXT REVIEW DATE: *9/2/2015*

1. AUTHORITY

- 1.1 New Mexico State Statute 9-27-1 et seq. NMSA 1978 Department of Information Technology Act

2. REFERENCES

- 2.1 Procurement Code, NMSA 1978, Sections 13-1-28 through 13-1-199.
- 2.2 Public Records Act, NMSA 1978, Section 14-3-1 et seq.
- 2.3 State Personnel Board Rule, 1 NMAC 7, 11 Discipline
- 2.4 State of New Mexico Information Security Policy
- 2.5 Department of Information Technology Policy 361-03 Code of Conduct
- 2.6 Information Technology Rule, NMAC 1.12.10 Internet, Intranet, Email, and Digital Network Usage

3. PURPOSE:

This policy describes the secure and acceptable usage of State issued mobile devices.

4. SCOPE

All State of New Mexico employees that use state issued mobile devices.

Within scope is the acceptable use of State issued mobile phones, Personal Digital Assistants, Blackberry, Android phones, iPhones, MS Windows phones, smart

phones, iPads, tablets and similar portable devices which are able to connect to the internet.

Not within scope are two-way radios, jump drives, desktop computers, netbook computers or laptop computers.

5. BACKGROUND

N/A

6. DEFINITIONS

- 6.1 Agency: A department, commission, board, or institution of the State of New Mexico
- 6.2 Apps: Applications that are installed on a mobile device
- 6.3 Authorized user: any user who has permission given by an agency to use the mobile device, typically authorized user is limited to the employee to whom the device is issued to by their agency, and as necessary the employee's direct supervisor, agency ITO staff and DoIT staff.
- 6.4 CIO: Chief Information Officer
- 6.5 Contractor: A person that is not a state employee and has or is working with someone who has (sub-contractor) an active contract with the DoIT or any agency
- 6.6 Direct Supervisor: The designated supervisor or manager that an employee reports to; which directs and oversees the employee's position requirements
- 6.7 DoIT: Department of Information Technology
- 6.8 Employee(s): State of New Mexico employee(s) who work for the DoIT or work for an agency that the DoIT provides enterprise services to
- 6.9 Executive Branch: State of New Mexico Executive Branch
- 6.10 "Floater" devices: A device that is not assigned to a specific person but is used by multiple employees or by a contractor
- 6.11 "Jail Broken" or "Rooting": Altering the device operating system for the purpose of removing or circumventing restrictions
- 6.12 Mobile Device(s): Includes but is not limited to state issued cell phones, smart phones, tablets or other portable devices that have the ability to connect to the internet via a cellular, Wi-Fi or other wireless network.

- 6.13 Multimedia: Includes but is not limited to pictures, video, music, and voice recordings
- 6.14 Messages: Includes but is not limited to Short Message Service (SMS) messages, emails, Multimedia Message Service (MMS) messages, Blackberry Messenger (BBM), iMessages, and services provided through social media sites
- 6.15 Service Catalog: The central repository of DoIT services which includes detailed service descriptions, pricing, service options, support and provisioning information and service levels
- 6.16 Passwords: String of characters used for authenticating a user on a mobile device. Passwords are private to each user. May also be referred to as passcode, lock code or access code.
- 6.17 SPO, State Personnel or Personnel Office : State of New Mexico Personnel Office
- 6.18 Relevant Agency Head: The agency Cabinet Secretary, Deputy Secretary, or Division Director
- 6.19 Securely Stored: reasonable measures taken to physically protect the device from theft or unauthorized use
- 6.20 State: State of New Mexico
- 6.21 User(s): State employee or contractor issued a mobile device for state business use

7. POLICY

- 7.1 DoIT is the single and consolidated cellular, data and phone service provider for the executive branch. All executive branch agencies are required to procure these services through DoIT.
- 7.2 Appropriate Usage
- 7.2.1 The responsibility for the appropriate use of mobile devices rests with the designated user. The relevant agency head and agency CIO are responsible for providing relevant policy and procedure information to their users. Users are responsible for reading and abiding by the provided rules and policies upon receipt of a mobile device.
- 7.2.2 Users shall have no expectation of privacy with respect to a mobile device. There is no expectation of privacy in apps installed, multimedia or data located on the mobile device, usage, and messages in any form sent to or from.

- 7.2.3 All mobile devices are the property of the state, and are provided for employees' legitimate business use. Additionally, any alteration of a mobile device's operating system is prohibited and thus shall not be "jail broken" or "rooted" by any user.
- 7.2.4 As property of the state, any apps installed on the mobile device should not be through a user's personal account, i.e. an iTunes account, or gmail account. Where such an account is required for state business, separate accounts associated with the employee's state email shall be created.
- 7.2.5 Incidental personal use is acceptable as long as it does not interfere with state business and is consistent with applicable state and/or agency policies and rules. DoIT and agencies have the authority to limit personal or incidental uses of any mobile device.
- 7.2.6 Users shall not use, try to use, or let anyone else use mobile devices for: anything that is illegal; making offensive, threatening or harassing calls; or messaging or emailing inappropriate or offensive remarks, graphics or images.
- 7.2.7 Mobile devices shall only be used by authorized users. Internet, Intranet, Email, and Digital Network Usage rule; enterprise security policies and rules; agency code of conduct policy; and State and/or agency personnel rules apply to mobile devices.
- 7.2.8 A specific employee name must be associated with every mobile device. For "floater devices", a manager or direct supervisor's name must be associated with that device.

7.3 Mobile Device Security

- 7.3.1 DoIT has the authority to install software to secure mobile devices consistent with this policy and ensure appropriate state business usage.
- 7.3.2 All mobile devices must have a password enabled. The device must be set to lock no later than 15 minutes after inactivity.
- 7.3.3 The loss of mobile devices that can send, store and retrieve email or access DoIT or State information systems has potentially serious repercussions for the State because of the sensitivity of the information that may be stored on them. All losses of mobile devices must be formally reported to the employee's manager or direct supervisor the agency CIO and the DoIT service desk within 24 hours. The phone number for a lost or stolen phone will be immediately disabled.
- 7.3.4 All broken, damaged, or malfunctioning mobile devices must be reported within 24 hours to the employee's manager or direct supervisor for replacement or repair.

7.3.5 Confidential or sensitive information, client data, or other information covered by existing state or federal privacy or confidential laws, regulations, rules, policies, procedures, or contract terms, to the greatest extent possible, should not be stored on mobile devices. Sensitive information, if stored on mobile devices, shall be securely encrypted. Sensitive and critical data or information stored on a mobile device shall not be the only instance of the data. Additionally, sensitive information must be transmitted in a secure fashion.

7.3.6 Mobile devices must be securely stored when not in use. Covers should be used to provide a degree of physical protection, and may be requested. Users may be liable for repair or replacement costs, should their mobile device be damaged or lost.

7.4 Agencies shall have the authority to establish an agency specific mobile device security and usage policy, which references this policy. Such policy must at a minimum abide by all requirements set forth in this policy.

8. PROCEDURES

8.1 Procedures for mobile devices and services are located in the DoIT Service Catalog.

9. FORMS

Forms related to this policy may be found in the DoIT Service Catalog.

10. MANAGEMENT:

10.1 The State CIO may allow necessary changes or exceptions to this policy.

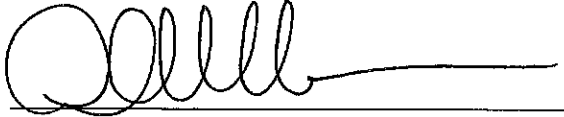
10.2 It is the responsibility of the DoIT Enterprise Services to assure the Service Catalog is up to date and reflective of this policy.

10.3 Appropriate and timely notification will be made regarding change(s) in policy or procedures, as deemed appropriate by the State CIO.

10.4 Each reported infraction of this policy will be handled on its own merit and may be subject to disciplinary action in conjunction with applicable agency and state rules and policies.

10.5 The DoIT will review this policy annually in accordance with the DoIT Policy Management Plan.

11. APPROVAL:

A handwritten signature in black ink, consisting of a large 'D' followed by several loops and a long horizontal stroke at the end, positioned above a horizontal line.

Darryl Ackley
Cabinet Secretary and State Chief Information Officer
Department of Information Technology

9/2/2014

Date