DocuSign Envelope ID: 6B73EF20-BEE6-40C3-A895-695BE2BCD8CA

NM DEPARTMENT OF INFORMATION TECHNOLOGY

Michelle Lujan Grisham
New Mexico Governor

Raja Sambandam
Acting Cabinet Secretary & State CIO

Policy Title:	**Enterprise Mobile Device Security and Usage Policy**
Policy Number:	**DoIT-361-710**
Effective Date:	**3/21/22**
Issued By:	**DoIT CIO**
Distribution:	**DoIT IT Resource Users**
Approved by:	**Raja Sambandam, Acting Cabinet Secretary**

1. AUTHORITY

Pursuant to the New Mexico Department of Information Technology Act, NMSA 1978, § 9-27-1 *et seq.*, the Secretary of the Department of Information Technology (DoIT or Department) shall exercise general authority over all department employees, manage all operations of the Department, and administer and enforce the laws with which the Secretary or the Department is charged.

2. PURPOSE

This policy describes the secure and acceptable usage of State of New Mexico-issued mobile devices, tablets, or other portable devices with ability to connect to the Internet via a cellular, Wi-Fi, or another network.

3. SCOPE

This Policy applies to all State of New Mexico employees who use State-issued mobile devices, including mobile phones based on Blackberry OS, Android OS, Apple iOS, Microsoft Mobile OS, or other smart phone operating systems.

4. DEFINITIONS

a. **DoIT IT Resource Users** - All DoIT employees, contractors, and any other users of DoIT information technology (IT) resources.
b. **Apps** – Applications installed on a mobile device.
c. **Authorized User –** Any user who has DoIT's permission to use a State- issued mobile device.
d. **Floater Devices –** Devices not assigned to a specific person, but that are used by multiple individuals.
e. **Jail Broken or Rooting –** Altering a mobile device operating system to remove or circumvent restrictions.
f. **Messages –** Include, but are not limited to, Short Message Services (SMS), emails, Multimedia Message Service (MMS), Blackberry Messenger (BBM), iMessage's, and communications services provided through social media sites.

DocuSign Envelope ID: 6B73EF20-BEE6-40C3-A895-695BE2BCD8CA

5. POLICY

Only Authorized Users may use State-issued mobile devices. Internet, intranet, email, and digital network usage rules; enterprise security policies and rules; agency code of conduct policies; and State and/or agency personnel rules apply to State-issued mobile devices.

Individuals using State-issued mobile devices shall have no expectation of privacy with respect to their use of such devices, including installed apps, multimedia usage and/or messages in any formsent or received, or data located on the device.

All State-issued mobile devices remain the property of the State. They are provided strictly for legitimate State business use. Any alteration of a mobile device's operating system is prohibited, and such devices shall not be "jail broken" or "rooted" by any user.

Mobile device security requirements:

- **a.** Each State-issued device must be assigned to a specific, named Authorized User; floater devices must be assigned to a manager or supervisor within the organization sharing the floater device;
- **b.** All mobile devices must be password protected; and
- **c.** All mobile devices must be set to lock after no more than 1 minute of inactivity and mustlock instantly after users turns off the mobile device screen.

To the greatest degree possible, users shall not store on a State-issued mobile device any confidential or sensitive information or client data, or other information covered by existing State or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms. If such information is stored on a mobile device, the information must be securely encrypted and must not be the only copy of the data. Any such information transmitted using a mobile device must be transmitted in a secure fashion compliant with approved encryption methods.

The loss of mobile devices that can send, store, and/or retrieve email or access DoIT or other State information systems has potentially serious repercussions for the State due to sensitivity of information that is stored. In the case of a lost or stolen phone or other mobile device, DoIT Mobile Device Administrator(s) will immediately disable the device remotely upon notification that the device is lost or stolen.

All DoIT IT Resource Users, including mobile device users, are subject to DoIT's *Acceptable Use of IT Resources Policy*. When DoIT authorizes use of a non-State-owned application that may only be sourced from an application marketplace (e.g., Google PlayStore, Apple App Store), any required 3rd party account ID must match the issued user's "@state.nm.us" format wherever possible, to ensure consistent accountability.

Mobile devices provided by DoIT will be decommissioned and sanitized as per DoIT's *DataClassification Policy* and *IT Change Management Policy*.

DocuSign Envelope ID: 6B73EF20-BEE6-40C3-A895-695BE2BCD8CA

6. ROLES AND RESPONSIBILITIES

a. DoIT Executive Management

DoIT executive management (DoIT Chief Information Officer (CIO), Chief Information Security Officer (CISO), or CIO designee) is responsible for implementing this Policy. The DoIT CISO or CIO designee will ensure development, documentation, updates, and distribution of information necessary to protect the security of State-issued mobile devices.

b. Authorized Users

i. Are responsible for reading and complying with DoIT mobile device usage-related policies and procedures;
ii. Are responsible for appropriate use of mobile device(s) in their possession;
iii. Shall not install any apps through a personal account (e.g., iTunes, Gmail).
iv. Shall take reasonable measures to physically protect the device from theft orunauthorized use;
v. May use State-issued mobile devices for incidental personal use only if suchusage does not interfere with State business and is consistent with applicable State and/or DoIT policies and rules, including but not limited to DoIT's Acceptable Use of IT Resources Policy;
vi. Shall not allow anyone else to use State-issued mobile devices for other than legitimate State or DoIT business purposes constitute a violation of State or DoIT policy if;
vii. Shall formally report the loss of any State-issued mobile device to the user's direct supervisor via written e-mail, to the agency CISO and CIO, and to the DoIT Helpdesk as soon as possible and in no event longer than 24 hours of realizing the device is missing;
viii. Shall store State-issued mobile devices securely when not in use;
ix. May request that DoIT provide a cover for a mobile device to provide a degree ofphysical protection; and
x. May be subject to disciplinary action, up to and including termination of employment, should the State- issued mobile device be damaged or lost due to the user's fault.

c. Supervisors

Supervisors will oversee the responsible use of State-issued mobile devices by their staff.

d. DoIT Helpdesk

DoIT Helpdesk shall create a ticket upon notification of mobile device loss or malfunctionand shall assign the ticket to the DoIT Telecommunications team.

e. DoIT Mobile Device Administrator

DoIT mobile device administrators shall track orders and devices issued to users.

DocuSign Envelope ID: 6B73EF20-BEE6-40C3-A895-695BE2BCD8CA

f. CIO or CISO

DoIT's CIO, CISO, or CIO designee:

i. Are responsible for establishing and enforcing relevant policies and procedures, and ensuring DoIT IT Resource Users are aware of their requirements; and have the authority to limit personal or incidental use of any mobile device.

ii. Have the authority to install software to secure mobile devices, consistent with this Policy, and to ensure appropriate State business usage; and

iii. Shall ensure encryption standards and security configurations of mobile device areapplied and maintained.

NMAC 1.12.20.27 PORTABLE DEVICES AND REMOVABLE MEDIA:

A. All state-owned portable computing resources and removable media shall be secured to prevent compromise of confidentiality or integrity of information. All portable computing devices and removable media must be protected by a password.

B. No portable and removable media computing devices may store or transmit sensitive information without suitable protective measures approved by the agency CIO.

C. An agency user of portable computing devices such as notebooks, PDAs, laptops, and mobile phones, Smartphones, or any other such then current portable devices, shall obtain the approval from the agency CIO to use and such approval shall be based on satisfactory documentation that the requirements for physical protection, access controls, cryptographic techniques, back-ups, malware and malicious codes protection and the rules associated with connecting portable devices to networks and guidance on the use of these devices in public places have been met.

D. Agency users shall be instructed that when using portable computing devices or removable media in public places, meeting rooms and other unprotected areas outside of the agency's premises, they must use appropriate protection, such as using cryptographic techniques, firewalls, and updated virus protection shall be in place to avoid the unauthorized access to or disclosure of the agency information stored and processed by these devices.

E. Agency users shall be instructed that when such portable devices or removable media are used in public places care shall be taken to avoid the risk of unauthorized persons viewing on-screen sensitive or protected information.

F. Procedures protecting portable devices or removable media containing sensitive information against malicious software shall be developed, implemented, and be kept up-to-date.

G. Portable devices and removable media containing sensitive or protected information shall be attended at all times and shall be secured e.g., do not leave devices unattended in public places.

H. Agency shall provide training to all staff using portable devices and removable media to raise their awareness with respect to risks resulting from the use of portable devices and removable media and what controls are in place by the agency to protect state data and equipment.

DocuSign Envelope ID: 6B73EF20-BEE6-40C3-A895-695BE2BCD8CA

I. Employees in the possession of portable devices and removable media shall not check such items in airline luggage systems or leave in unlocked vehicles. Such devices shall remain in the possession of the employee as carry-on luggage unless other arrangements are required by federal or state authorities.

J. In the event a state-owned portable device or removable media is lost or stolen; it is the responsibility of the user of that device to immediately report the loss following procedures in 1.12.20.34 NMAC.

NMAC 1.12.20.34 LOST OR STOLEN IT ASSET:

In the event of a lost or stolen IT asset, the user shall:

A. immediately report the incident to the user's supervisor;
B. immediately report the incident to the DoIT help desk at (505)827-2121 or EnterpriseSupportDesk@state.nm.us; a state IT asset incident form must be completed and signed by the agency CIO and returned to the DoIT help desk; the asset incident form can be found on the DoIT security web site at: http://www.doit.state.nm.us/securityoffice.html;
C. if stolen, user must contact the local law enforcement agency to report the theft and receive a crime report case number;
D. upon loss of or in the event of loss of an IT asset by theft, the agency CIO shall work with the DoIT CISO to identify the nature of the data exposed; the loss of confidential or sensitive data shall be reported to the agency executive management for direction.
[1.12.20.34 NMAC - N/E, 04/14/2010]

7. EXCEPTIONS

The DoIT CIO or CISO must approve in advance and in writing any exception to this Policy.

8. VIOLATIONS

Any DoIT IT Resource User found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

9. REFERENCES

a. National Institute of Standards and Technology 800-124 r1, Guidelines forManaging the Security of Mobile Devices in the Enterprise
b. National Institute of Standards and Technology Special PublicationSP800-53 r4: AC-19, AC-19(5), MP-5(4), MP-6, MP-6(1), PL-4(1)
c. Department of Information Technology Customer I.S. Policy
d. Department of Information Technology Data Classification Policy
e. Department of Information Technology Acceptable Use Policy

DocuSign Envelope ID: 6B73EF20-BEE6-40C3-A895-695BE2BCD8CA

10. CHANGE HISTORY

Date	Version	Changed By	Change Comments
09/30/2019	1		Initial Draft
09/30/2020	2		Revision Draft
02/26/2021	3	Raja S	Revised and routed for Union approval
06/29/2021	4	Olga Serafimov, Esq.	Reviewed and revised for legal compliance
10/13/2021	5	Brenda Fresquez	Reviewed for quality assurance
03/15/2022	6	Marko Satarain	No changes, reviewed and accepted by HR—Marko Satarain, Legal—Todd Baran and CWA—Dan Secrist

Approval

DocuSigned by:
437214FBE82C453...

3/21/2022

Raja Sambandam, Acting Cabinet Secretary **Date**