



ANDREW M. CUOMO  
Governor

State Capitol P.O. Box 2062  
Albany, NY 12220-0062  
[www.its.ny.gov](http://www.its.ny.gov)

BRIAN DIGMAN  
NYS Chief Information Officer  
Director, Office of IT Services

<b>New York State Information Technology Standard</b>	<b>No:</b> NYS-S14-009
<b>IT Standard:</b>  Mobile Device Security	<b>Effective:</b> 04/18/2014
	<b>Issued By:</b> NYS ITS  <b>Standard Owner:</b> Enterprise Information Security Office

## 1.0 Purpose and Benefits of the Standard

---

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices that are only used within a State Entity's (SE) facilities and on the SE's networks.

This standard outlines the additional protections required for the use of mobile devices by SEs.

## 2.0 Enterprise IT Policy/Standard Statement

---

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services, the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information (IT) Policy, Standards and Guidelines.

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/policy/glossary.htm>.

## 3.0 Scope

---

This standard covers all mobile devices issued or managed by the State or which are used by the State workforce to store SE information.

Mobile devices are computing devices in a small form factor that have at least one network connection interface, non-removable and/or removable storage, and is portable (i.e., non-stationary). These devices come in the forms such as: smartphones, PDAs, smart watches, tablets, laptops, and wearable devices.

## 4.0 Information Statement

---

- 4.1. Mobile devices must follow all requirements of the [NYS Information Security Policy](#).
- 4.2. As per the state [Encryption Standard](#), all mobile devices that access or contain any SE information must be encrypted.
- 4.3. For State issued mobile devices or personal mobile devices with direct access to NYS-managed networks, only those applications which are approved by the SE may be installed and or run on the mobile devices. Applications must be restricted through the use of whitelisting (preferable) or blacklisting. Applications must be digitally signed to ensure that only applications from trusted entities are installed on the device and that code has not been modified.
- 4.4. State information must be removed from mobile devices (e.g., wiping, removing access to the State container) after no more than 10 incorrect authentication attempts.
- 4.5. Mobile devices must automatically lock after being idle for a period not to exceed 10 minutes.
- 4.6. Mobile devices which directly connect to NYS-managed private networks, virtually connect to NYS-managed private networks in a manner consistent with a directly connected device, or which contain or could contain SE information, including e-mail data, must be managed by a Mobile Device Management (MDM) or other centralized management solution.
- 4.7. Use of synchronization services, such as backups, for mobile devices (e.g., local device synchronization, remote synchronization services, and websites) must be controlled by the SE through an MDM or other centralized management solution.
- 4.8. Mobile devices may not access NYS private networks unless their software integrity is verified (including whether the device has been rooted/jailbroken).
- 4.9. The MDM or other centralized management solution must be able to enforce the following SE optional security policies and the enterprise security policies detailed in 4.1-4.8 above:
  - a. Restrict user and application access to hardware, such as the digital camera, GPS, Bluetooth interface, USB interface, and removable storage, in accordance with SE requirements.
  - b. Restrict user and application access to the built-in web browser, e-mail client, application installation services, text messaging, etc., in accordance with SE requirements.

4.10. SEs must manage all mobile devices by:

- a. Implementing device policies and configurations as appropriate to the use of the device.
- b. Developing and implementing processes which check for upgrades and patches to the software components, and for appropriately acquiring, testing, and deploying the updates to State issued devices.
- c. Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.
- d. Detecting and documenting anomalies which may indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators as appropriate.
- e. Providing training and awareness activities for mobile device users on threats and recommended security practices which can be incorporated into the SE's security and awareness training.

## 5.0 Compliance

---

This standard shall take effect upon publication. The Policy Unit shall review the standard at least once every two years to ensure relevancy. The Office may also assess agency compliance with this policy. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber, or Legislative entities.

Assessments will be performed periodically to confirm that the SE's mobile device processes and procedures are being followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, SEs shall request an exception through the Enterprise Information Security Office exception process.

## 6.0 Definitions of Key Terms

---

**Mobile Device** A computing device in a small, portable form factor that has at least one network connection interface, non-removable and/or removable storage, including but not limited to smartphones, Personal Digital Assistants (PDAs), tablets, laptops, smart watches, and wearable devices.

## 7.0 ITS Contact Information

---

Submit all inquiries and requests for future enhancements to the standard owner at:

**Standard Owner**  
**Attention: Enterprise Information Security Office**  
**New York State Office of Information Technology Services**  
**State Capitol, ESP, P.O. Box 2062**  
**Albany, NY 12220**  
**Telephone: (518) 242-5200**  
**Facsimile: (518) 322-4976**

Questions may also be directed to your ITS Customer Relations Manager at:  
[Customer.Relations@its.ny.gov](mailto:Customer.Relations@its.ny.gov)

The State of New York Enterprise IT Policies may be found at the following website:  
<http://www.its.ny.gov/tables/technologypolicyindex.htm>

## 8.0 Review Schedule and Revision History

---

Date	Description of Change	Reviewer
04/18/2014	Original Standard Release	Thomas Smith, Chief Information Security Officer
04/18/2015	Scheduled Standard Review	

## 9.0 Related Documents

---

- [NIST Special Publication 800-124, Guidelines for Managing and Securing Mobile Devices in the Enterprise](#)
- [NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices](#)
- [Federal CIO Council and Department of Homeland Security Mobile Security Reference Architecture](#)