NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	**No:** NYS-S14-009
IT Standard: **Mobile Device Security**	**Updated:** 08/16/2021
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

Mobile devices often need additional protection because by their nature, these devices generally have a higher exposure to threats when compared to SE 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 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117*[1], established January 2002, provides the State Chief Information Officer with 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 Technology (IT) Policy, Standards and Guidelines*.

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002, and continued by Executive Order 5 issued by Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, and Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011.

3.0 Scope

This standard applies to all "State Entities" (SE), defined as "State Government" entities as defined in Executive Order 1171, issued January 2002, or "State Agencies" as defined in Section 101 of the State Technology Law including their employees, and all third parties (e.g., local governments, consultants, vendors, and contractors), that use or access any IT resource for which the SE has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. While an SE may adopt a different standard, it must include the requirements set forth in this one.

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

4.0 Information Statement

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 are portable. These devices come in many forms and names including smartphones, Personal Digital Assistants (PDAs), tablets, laptops, smartwatches, and wearable devices. Mobile devices must follow all requirements of the NYS-P03-002 Information Security Policy and the following:

1. As required by the NYS-S14-007 Encryption Standard, all mobile devices that access or contain any SE information must be encrypted.
2. For State-issued mobile devices or personal mobile devices with direct access to SE private networks (*see* NYS-S14-012 Bring Your Own Device Standard), only those applications which are approved by the SE may be installed and/or run on the mobile devices. Controls must be in place to both enforce SE application control requirements and prevent the installation of unauthorized or prohibited applications. Applications accessing SE data must be delivered either through the platform vendor's AppStore or State-authorized management systems.
3. SE information must be removed or rendered inaccessible from mobile devices after no more than 10 incorrect authentication attempts.
4. Mobile devices must automatically lock after being idle for a period not to exceed 10 minutes.
5. Mobile devices which directly connect to SE private networks or virtually connect to SE private networks in a manner consistent with a directly connected device must be managed by a Mobile Device Management (MDM) or other centralized management solution.
6. Mobile devices which contain or may contain SE information must be managed with MDM or other centralized management solution, or access to the SE information must be made via applications controlled with a Mobile Application Management (MAM) solution.

7. Use of mobile device synchronization services, including backups (e.g., local device synchronization, remote synchronization services, and websites) must be controlled by the SE through an MDM or other centralized management solution.
8. The mobile device's operating environment integrity must be verified (including whether the device has been rooted/jailbroken) prior to accessing SE private networks
9. SEs must manage all mobile devices by:
    a. Implementing mobile device policies and configurations as appropriate to the use of the mobile device.
    b. Developing and implementing processes that check for upgrades and patches to the mobile device's software components, and for appropriately acquiring, testing, and deploying the updates to State-issued mobile devices, when technically possible.
    c. Providing a mechanism to quarantine, or otherwise isolate, a mobile device from SE private networks or applications if it is below a minimum OS version or software patch level.
    d. Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.
    e. Detecting and documenting anomalies that may indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators as appropriate.
    f. Providing training and awareness activities for mobile device users on threats and recommended security practices that can be incorporated into the SE's security and awareness training.

5.0 Compliance

This standard shall take effect upon publication. Compliance is required with all ITS policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

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

6.0 Definitions of Key Terms

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

7.0 Contact Information

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

Chief Information Security Office
Reference: NYS-S14-009
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This standard shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
04/18/2014	Original Standard Release	Thomas Smith, Chief Information Security Officer
05/15/2015	Minor clarifications, added link to the BYOD standard and removed optional language pertaining to MDM	Deborah A. Snyder, Deputy Chief Information Security Officer
02/15/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
09/11/2018	Scheduled review – minor change to relocate a paragraph from Scope to Information Statement, Authority, Scope and title of office	Deborah A. Snyder, Chief Information Security Officer
08/16/2021	Review and minor updates	Karen A. Sorady, Chief Information Security Officer

9.0 Related Documents

NIST Special Publication 800-124, Rev 1, Managing the Security of Mobile Devices in the Enterprise

Department of Homeland Security (DHS) Science & Technology (S&T) Directorate Mobile Device Security