



# Office of Information Technology Services

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

|  |  |
|--|--|
| <b>New York State Information Technology Standard</b>    | <b>No:</b> NYS-S14-009   |
| <b>IT Standard:</b><br><br><b>Mobile Device Security</b> | <b>Updated:</b> 08/18/2025   |
|  | <b>Issued By:</b> NYS Office of Information Technology Services<br><br><b>Owner:</b> Chief Information Security Office |

## 1.0 Purpose and Benefits

Mobile devices often need additional protection due to a higher risk of exposure to threats when compared to State Entity (SE) devices that are only used within an SE’s 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<sup>1</sup> 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.

<sup>1</sup> 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 Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011, and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

## 3.0 Scope

---

This standard applies to all “State Entities,” defined as “State Government” in Executive Order 117 or “State Agencies” as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any Information technology (IT) Resource for which the SE or ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE or ITS. While an SE may adopt a different standard, it must include the requirements set forth in this one. Where a conflict exists between this standard and an SE’s standard, the more restrictive standard will take precedence.

## 4.0 Information Statement

---

Mobile devices are portable computing devices in a small form factor that an individual can easily carry. They are designed to operate without a physical connection, feature non-removable and/or removable data storage, and have a self-contained power source, along with input and output capabilities, excluding laptops and/or small form factor workstations. These devices come in many forms and names including smartphones, tablets, smartwatches, and wearable devices. Mobile devices must adhere to all requirements in the [NYS-P03-002 Information Security Policy](#), and its associated standards, in addition to the requirements in this standard:

All mobile devices that contain SE information must be managed in accordance with SE policy and procedures including:

1. Implementing mobile device policies and configurations as appropriate to the use of the mobile device.
2. 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.
3. Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.
4. Detecting and documenting anomalies that may indicate malicious activity or deviations from policy and procedures. Anomalies should be reported in accordance with the SE’s approved reporting policies and procedures.
5. 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.
6. Applications accessing SE information must be delivered through an authorized application management system.

### 4.1 Mobile Device Management (MDM)

All mobile devices which contain or may contain SE information, or access SE internal networks, must be managed with MDM or other centralized management solutions.

MDM solutions must be configured to provide the following controls:

1. Mobile devices must automatically lock after being idle for a period not to exceed 10 minutes.
2. Where technically feasible, controls must be implemented to allow for remote wiping of lost or stolen mobile devices.
3. SE information must be removed or rendered inaccessible from mobile devices after no more than 10 incorrect authentication attempts.
4. The mobile device's operating environment integrity must be verified, including whether the device has been rooted/jailbroken.
5. 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.
6. Ensure devices are encrypted as required by the [NYS-S14-007 Encryption Standard](#).
7. Provide 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.
8. Ensure that only those applications which are approved by the SE may be installed and/or run on the mobile devices.

## 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 the [ITS 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**  
**31 British American Blvd.**  
**Latham, NY 12110**  
**Telephone: (518) 242-5200**  
**Email: [CISO@its.ny.gov](mailto:CISO@its.ny.gov)**

Statewide technology policies, standards, and guidelines may be found at the following website: <https://its.ny.gov/policies>.

## 8.0 Revision History

---

This policy document should be reviewed consistent with the requirements set forth in ITS-P24-003 Process for Establishing Information Technology Policies, Standards, and Guidelines.

| <b>Date</b> | <b>Description of Change</b>  | <b>Reviewer</b>   |
|-------------|---|---|
| 04/18/2014  | Original Standard Release   | Thomas Smith,<br>Chief Information<br>Security Officer                |
| 05/15/2015  | Minor clarifications, added link to the BYOD standard and removed optional language pertaining to MDM                             | Deborah A. Snyder,<br>Deputy Chief<br>Information Security<br>Officer |
| 02/15/2017  | Update to Scope, contact information and rebranding   | Deborah A. Snyder,<br>Deputy Chief<br>Information Security<br>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,<br>Chief Information<br>Security Officer           |
| 08/16/2021  | Review and minor updates  | Karen A. Sorady,<br>Chief Information<br>Security Officer             |
| 08/18/2025  | Scheduled review – updated Scope and Authority language. Reorganization of Information Statement and minor language changes.      | Chris DeSain,<br>Chief Information<br>Security Officer                |

## 9.0 Related Documents

---

[NIST SP 800-124, Rev. 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise](#)

[Department of Homeland Security \(DHS\) Science & Technology \(S&T\) Directorate](#)

[Mobile Device Security](#)

[NYS-S14-011 Enterprise Mobile Management](#)