



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-S14-012
IT Standard: Bring Your Own Device (BYOD)	Updated: 11/29/2017
	Issued By: NYS Office of Information Technology Services Standard Owner: Chief Technology Office

1.0 Purpose and Benefits

The purpose of this technical standard is to normalize the management and administration of personal devices accessing state resources.

2.0 Authority

Section 103.10-11 of State Technology Law provides the Office of Information Technology Services (ITS) the authority to establish statewide technology policies, including technology standards and security. *Section 2 of Executive Order No. 117* provides the State Chief Information Officer, 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*.

3.0 Scope

This standard applies to ITS, all State Entities (SE) that receive services from ITS, and affiliates of same (e.g., contractors, vendors, solution providers), which have access to or manage SE information. It also serves as recommended practice for the State University of New York, the City University of New York, non-Executive branch agencies, authorities, NYS local governments and third parties acting on behalf of same.

This standard applies to all administrators of BYOD programs.

BYOD devices in scope for this standard include computers, smartphones, tablets and other devices running a mobile operating system, including but not limited to Android, BlackBerry OS, iOS, Linux, Mac OS X, Windows and Windows Mobile.

4.0 Information Statement

This standard identifies four methods of accessing state data and the level of management required:

4.1 Viewer-based Access

Users can access State managed data via a web, virtual desktop, or other interface. The data in this level does not reside on the device; no state management of the device is required. (Example, a home PC logging into a State Entity (SE) website to obtain information, either public or personally accessible to the user.)

4.2 Application Access

In the application model, all access to State data from the BYOD device is delivered via applications, which securely isolate State data from personal data on the device. Examples include virtual desktop infrastructure (VDI) or terminal clients that do not store State data, web browsers, or applications that encrypt data stored on the BYOD devices. (Example, a worker accesses a SE managed desktop (physical or virtual) with an SSL VPN client. SE manages the device and access method.)

Applications used in this manner must have the following capabilities:

1. Applications must not store plaintext state data on the BYOD device. Any State data stored on the device must be stored in a manner consistent with relevant security policies and encryption standards.
2. Applications must disallow access to State data to other applications on the device, unless access is secured in a manner consistent with relevant security policies and encryption standards.
3. The application or platform must have the ability to detect “jail broken” or “rooted” devices or similar mechanisms that bypass the platform security model and perform remediation.

4.3 Native Messaging and Calendar Access

In the messaging access model, end users are authorized to connect BYOD devices to State messaging platforms, using protocols such as Exchange ActiveSync or Outlook Web Access (OWA).

To allow this type of connectivity, BYOD devices must have the following capabilities:

1. Owners of the BYOD device must agree to allow the State to take intrusive measures to manage and protect State data, including the installation of software for device management. Device management software includes password policy, usage monitoring and remote wipe capability. These measures will impact personal data on the device.
2. The BYOD device must encrypt all State data in a manner consistent with relevant security policies and encryption standards.

3. Owners of the BYOD device must agree to be responsible for the use of the device, and to not allow others to use it without direct supervision.

4.4 Managed Device Access

In the managed device model, for cases where direct access to ITS-managed networks is required, BYOD devices are authorized to connect to State networks. Authorized devices will be managed in a manner identical to a State-owned device.

1. All devices must be compliant with enterprise baseline security requirements, and optional additional security controls specific to the SE that the device is assigned to.
2. Personal devices of this type must be managed in a manner consistent with the “Enterprise Mobile Management Technical Standard”.

5.0 Compliance

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

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, State Entities shall request an exception through the Enterprise 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 Technology Office
Reference: NYS-S14-012
New York State Office of Information Technology Services
Empire State Plaza
P.O. Box 2062 Albany, NY 12220
Telephone: 518-402-7000

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
04/11/2014	Issued standard	Chief Technology Office
10/6/2014	Formatting	Chief Technology Office
12/09/2016	Formatting	Chief Technology Office
11/29/17	Updated	Chief Technology Office

9.0 Related Documents

[NYS-P03-002 Information Security Policy](#)

[ITS-S07-001 ITS Encryption Standard](#)

[NYS-S14-009 Mobile Device Security Standard](#)