



ANDREW M. CUOMO
Governor

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

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

New York State Information Technology Standard	No: NYS-S14-012
IT Standard: Bring Your Own Device (BYOD)	Updated: 04/15/2014
	Issued By: NYS ITS – Office of the CTO Standard Owner: Kishor Bagul

1.0 Purpose

This technical standard is issued by the New York State Chief Technology Officer. The purpose of this technical standard is to normalize the management and administration of personal devices accessing state resources.

2.0 Scope

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.

3.0 Standard

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

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.)

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.

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.

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.”

4.0 Compliance

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 obtain written authorization of the Chief Technology Officer and Chief Information Security Officer.

5.0 Definitions

A complete listing of defined terms for NYS Information Technology Policies, Standards, and Best Practice Guidelines is available in the "NYS Information Technology Policies, Standards, and Best Practice Guidelines Glossary (<http://www.its.ny.gov/Policy/glossary.htm>).”

6.0 Contact Information

Office of the CTO Phone: 518-408-2484
Email: innovate@its.ny.gov

7.0 Revision History & Review Schedule

Date	Description of Change
04/11/14	Final Release
04/11/15	Scheduled Review

8.0 Related Documents

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

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