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-S14-012
IT Standard: **Bring Your Own Device (BYOD)**	**Updated:** 120/1/2020
	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) 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* 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*.

3.0 Scope

This standard applies to all "State Entities" ("SE"), defined as "State Government" entities in Executive Order 117 or "State Agencies" as defined in Section 101 of the State Technology Law. This includes employees and all other third parties (such as local governments, consultants, vendors, and contractors), that use or access any ITS resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS. While an SE may adopt a different standard, it must include the requirements set forth in this one.

This standard applies to all administrators of Bring Your Own Device ("BYOD") programs. The BYOD devices encompassed in the scope of this standard includes computers, smartphones, tablets and other personal devices that can access ITS Resources.

4.0 Information Statement

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

4.1 Viewer-based Access

In the viewer-based access model, users can access State data via web applications or ITS-managed interfaces (e.g., a home PC logging into a SE website to obtain information, either public or personally accessible to the user, such as accessing email through a webmail client). Since the data in this level does not reside on the BYOD device, no State management of the BYOD device is required.

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 BYOD device. Application 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 (e.g., a State employee accesses a SE managed desktop (physical or virtual) with a Secure Socket Layer Virtual Private Network (SSL-VPN) client). In this instance, the SE manages the BYOD 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 BYOD device must be stored in a manner consistent with relevant security policies and encryption standards.
2. Applications must disallow access to State data from other applications on the BYOD device, unless access is secured in a manner consistent with relevant security policies and encryption standards.

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 approved methods.

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 measures to manage and protect State data, including the installation of software for BYOD device management. These measures may impact personal data on the BYOD 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 BYOD device, and to not allow others to use it without direct supervision.

4.4 Managed Device Access

In the managed device model, a BYOD device has to be specifically authorized for use to connect to ITS-managed networks, i.e., have direct access to State data. Authorized devices will be managed in a manner identical to a State-owned device. Section 4.4 does not apply to systems that connect to ITS-managed Internet-only networks.

1. All BYOD 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. BYOD devices of this type must be managed in a manner consistent with the following standard: NYS-S14-011 Enterprise Mobile Management Technical Standard.

5.0 Compliance

This standard shall take effect upon publication. Compliance is required with all enterprise 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 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
12/01/2020	Updated content as well as scope and authority	Chief Technology Office

9.0 Related Documents

NYS-P03-002 Information Security Policy

NYS-S14-007 Encryption Standard

NYS-S14-009 Mobile Device Security Standard

NYS-S14-011 Enterprise Mobile Management