NEW YORK STATE OF OPPORTUNITY. | **Office of Information Technology Services**

New York State Information Technology Standard	**No:** NYS-S14-008
IT Standard: **Secure Configuration**	**Updated:** 09/11/2018
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

The purpose of this standard is to establish baseline configurations for information systems that are owned and/or operated by, or operated on behalf of, New York State (NYS). Effective implementation of this standard will maximize security and minimize the potential risk of unauthorized access to NYS information and technology.

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 as defined in Executive Order 117, established January 2002, 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 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 applies to all information systems owned and/or operated by, or operated on behalf of, NYS. Lab systems, such as those used for digital forensics or research, may require special consideration, however, this standard must be applied unless doing so inhibits the core functions of these systems or is otherwise not technically feasible.

4.0 Information Statement

Standard secure configuration profiles, based on any one or more of the industry consensus guidelines listed below, must be used in addition to the latest vendor security guidance. Alterations to the profile must be based on business need or NYS policy or standard compliance, developed in consultation with the Information Security Officer/designated security representative, documented and retained for audit purposes.

Industry Consensus Guidelines

- Center for Internet Security (CIS) Benchmarks

- Defense Information Systems Agency (DISA) Standard Technical Implementation Guidelines (STIG)

- National Institute of Science and Technology (NIST) National Checklist Program

- United States Government Configuration Baselines (USGCB)

- National Security Agency Security Configuration Guides

The initial setup, software installation, and security configuration of new systems must be performed in a secure environment isolated from other operational systems with minimal communication protocols enabled.

Changes to configuration are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation in accordance with the State Entity (SE) change management procedures. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to information systems and the associated security ramifications.

SEs must maintain configuration management plans that define detailed processes and procedures for how configuration management is used to support secure system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the secure system development life cycle.

A configuration monitoring process must be in place to identify undiscovered or undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes.

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 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-S14-008
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12242
Telephone: (518) 242-5200
Email: EISO@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 subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
04/18/2014	Original Standard Release	Thomas Smith, Chief Information Security Officer
05/15/2015	Minor clarification to initial system setup	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 changes to Authority, Scope, and title of office	Deborah A. Snyder, Chief Information Security Officer

Date	Description of Change	Reviewer
06/14/2021	Updated Scope	Karen Sorady, Chief Information Security Officer

9.0 Related Documents