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-S14-008
IT Standard: **Secure Configuration**	**Updated:** 02/29/2024
	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*[1], issued January 2002, 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*.

[1] 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” (SE), 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 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.

This standard applies to all information technology (IT) and operational technology (OT) systems owned and/or operated by, or operated on behalf of an SE.

4.0 Information Statement

Baseline security configuration profiles are used to implement hardened configurations on information systems and improve overall security. Baseline security configuration profiles must be implemented with least functionality (i.e., configuration of the information system to provide only essential capabilities) and reviewed at least annually. Profiles can include operating systems (OS), technology services, and software packages. These profiles must be based on one or more of the industry consensus guidelines listed below, in addition to the latest manufacturer or vendor security guidance:

- 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

Any changes to configurations or profiles must be formally identified, proposed, reviewed, documented, and retained for audit purposes. These changes must also be analyzed for security impact, tested, and approved prior to implementation in accordance with the SE’s change management procedures. Security impact analyses must be conducted by the SE ISO/designated security representative or a delegate with the necessary skills and technical expertise to analyze the changes to information systems and the associated security ramifications.

The initial setup, software installation, system updates, patching, and security configuration of new systems must be performed in a secure environment isolated from other operational systems with minimal communication protocols enabled. Patch management must be implemented per the NYS-S15-001 Patch Management Standard.

Per the NYS-S13-001 Secure System Development Lifecycle Standard, Appendix B Item 3, SEs must maintain configuration management plans that define detailed processes and procedures for how configuration management is used in conjunction with secure system development life cycle activities at the system level. Configuration management plans must include a maintenance schedule to refine and update configurations and profiles to adhere to the latest industry standards and hardening guidelines. Refreshing profiles could be driven by an updated benchmark or from an SE's updated or new security requirements. Configuration management plans must be maintained throughout the system's lifespan.

A configuration monitoring process must be in place to ensure system integrity (e.g., identifying undiscovered or undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes).

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 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 12226
Telephone: (518) 242-5200
Email: 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 NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

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
08/16/2021	Scheduled review – Minor wording changes for clarity and updating/removal of links to industry guidelines	Karen Sorady, Chief Information Security Officer
02/29/2024	Scheduled review – Updated Scope and Authority language, and minor wording changes	Chris Desain, Chief Information Security Officer

9.0 Related Documents

National Institute of Standards and Technology (NIST) 800-128, Guide for Security-Focused Configuration Management of Information Systems