



ANDREW M. CUOMO  
Governor

State Capitol P.O. Box 2062  
Albany, NY 12220-0062  
[www.its.ny.gov](http://www.its.ny.gov)

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

<b>New York State Information Technology Standard</b>	<b>No:</b> NYS-S14-008
<b>IT Standard:</b>  Secure Configuration	<b>Effective:</b> 04/18/2014
	<b>Issued By:</b> NYS ITS  <b>Standard Owner:</b> Enterprise Information Security Office

## 1.0 Purpose and Benefits of the Standard

---

The purpose of this standard is to establish baseline configurations for systems that are owned and/or operated by, or 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 Enterprise IT Policy/Standard Statement

---

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services, 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 (IT) Policy, Standards and Guidelines.

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/policy/glossary.htm>.

## 3.0 Scope

---

This standard applies to all systems owned and/or operated by, or 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](#)

Configuration, setup and initial software installation must be performed in a manner which minimizes the risk of system compromise prior to installation. For example, where appropriate and feasible, systems should be built in a secure network isolated from other operational systems with minimal communications protocols enabled.

Changes to configurations 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. The Policy Unit shall review the standard at least once every two years to ensure relevancy. The Office may also assess agency compliance with this policy. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber, or Legislative entities.

Assessments will be performed periodically to confirm that the SE's secure configuration processes and procedures are being followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing.

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 request an exemption through the Enterprise Information Security Office exception process.

## 6.0 Definitions of Key Terms

---

Not Applicable

## 7.0 ITS Contact Information

---

Submit all inquiries and requests for future enhancements to the standard owner at:

**Standard Owner**  
**Attention: Enterprise Information Security Office**  
**New York State Office of Information Technology Services**  
**State Capitol, ESP, P.O. Box 2062**  
**Albany, NY 12220**  
**Telephone: (518) 242-5200**  
**Facsimile: (518) 322-4976**

Questions may also be directed to your ITS Customer Relations Manager at:  
[Customer.Relations@its.ny.gov](mailto:Customer.Relations@its.ny.gov)

The State of New York Enterprise IT Policies may be found at the following website:  
<http://www.its.ny.gov/tables/technologypolicyindex.htm>

## 8.0 Review Schedule and Revision History

---

Date	Description of Change	Reviewer
04/18/2014	Original Standard Release	Thomas Smith, Chief Information Security Officer
04/18/2015	Scheduled Standard Review	

## 9.0 Related Documents

---

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