

---

Cyber Security Standard S10-001

**Role and Responsibilities of the State  
Entity Information Security Officer**

Original Publication Date: February 12, 2010  
Revision Date: July 30, 2010

---

**Thomas D. Smith  
Director  
New York State  
Office of Cyber Security  
30 South Pearl Street  
Albany, N.Y. 12207-3425**

## CYBER SECURITY STANDARD

Reference:	<b>S10-001, V1.1</b>
Standard Title:	<b>Role and Responsibilities of the State Entity Information Security Officer</b>
Related Policy:	<b>Cyber Security Policy P03-002, Information Security Policy</b>
Replaces & Supersedes:	<b>Cyber Security Standard S10-001, V1.0, February 12, 2010</b>
Authority:	<b>Section 715 of the Executive Law</b>
Issued By:	<b>Thomas D. Smith, Director, NYS Office of Cyber Security</b>
Original Publication Date:	<b>February 12, 2010</b>
Revision Date:	<b>July 30, 2010</b>

## **TABLE OF CONTENTS**

---

<b>TABLE OF CONTENTS</b> .....	<b>3</b>
<b>PURPOSE</b> .....	<b>4</b>
<b>SCOPE</b> .....	<b>4</b>
<b>STANDARD</b> .....	<b>5</b>
PREFACE .....	5
ROLE AND RESPONSIBILITIES OF THE STATE ENTITY INFORMATION SECURITY OFFICER .....	5
<i>Policy</i> .....	5
<i>Standard</i> .....	6
<b>DOCUMENT CHANGE MANAGEMENT</b> .....	<b>8</b>
<b>DEFINITIONS &amp; ACRONYMS</b> .....	<b>8</b>
<b>CONTACT INFORMATION</b> .....	<b>8</b>

## **PURPOSE**

---

The purpose of the Cyber Security Standards is to define a set of minimum security requirements that all *State Entities (SE)* must meet. These *Standards* shall serve as best practices for the State University of New York and the City University of New York campuses. Any *SE* may, based on its individual business needs and specific legal requirements such as the Health Insurance Portability and Accountability Act (HIPAA), exceed these security requirements, but must, at a minimum, achieve the security levels required by these *Standards*.

The primary objective of the Cyber Security Standards is to provide specific technical requirements. These *Standards* cover details such as implementation steps, *systems* design concepts, software interface mechanisms and other specifics.

## **SCOPE**

---

The Cyber Security Standards apply to all *SEs*. These *Standards* are not intended to unilaterally change the terms and conditions of employment. All *SEs*, when coming into compliance with these *Standards*, must consider all terms and conditions of employment including collective bargaining agreements.

These *Standards* are applicable to *SEs*, staff and all others, including outsourced *third parties*, which have access to or manage *SE information*. Where conflicts exist between these *Standards* and a *SE's standards*, the more restrictive *standards* will take precedence. The Cyber Security Standards for *SEs* encompass all *systems*, automated and manual, for which the *State* has administrative responsibility, including *systems* managed or hosted by *third parties* on behalf of the *SE*. It addresses all *information*, regardless of the form or format, which is created or used in support of business activities of *SEs*. These *Standards* must be communicated to all staff and all others who have access to or manage *SE information*.

## STANDARD

---

### Preface

The Cyber Security Standards are a statement of the minimum requirements, ethics, responsibilities and accepted behaviors required to establish and maintain a secure environment, and achieve the *State's information security* objectives. Compliance with these *Standards* is mandatory. The Cyber Security Standards set the direction, give specific guidance and define requirements for *information security* related processes and actions across *SEs*. These *Standards* document many of the security practices already in place in some *SEs*. Senior management is fully committed to *information security* and agrees that every person employed by or on behalf of New York State government has important responsibilities to continuously maintain the security of *SE data*.

Policies alone will not offer *SEs* the guidance necessary to implement the Cyber Security Policy and meet the objectives of the *State*. *Standards* provide this support and guidance by defining what is to be accomplished in specific terms. These *Standards* provide specific mandatory activities, actions, rules or regulations designed to reinforce **Cyber Security Policy P03-002**.

### Role and Responsibilities of the State Entity Information Security Officer (P03-002, Part 4. Organizational Security Policy)

#### Policy

The *SE* Information Security Officer (*ISO*) is responsible for performing, at a minimum, the following tasks:

- coordinate the development and implementation of *information security* policies, *standards*, procedures, and other control processes that meet the business needs of the *SE*;
- provide consultation for the various *SE* computing platforms;
- work closely with *security administration* or those serving in that function to ensure security measures are implemented to meet policy requirements;
- evaluate new security threats and counter measures that could affect the *SE* and make appropriate recommendations to the *SE's* Chief Information Officer and other management to mitigate the *risks*;
- review and approve all external network connections to the *SE's* network;
- provide consultation to the *SE* management with regard to all *information security*;
- investigate and report to appropriate internal management and the New York State Office of Cyber Security (OCS) according to the OCS Incident Reporting Policy P03-001;
- ensure that appropriate follow-up to security violations is conducted;
- ensure appropriate *information security* awareness and education to all *SE* employees, and where appropriate *third party* individuals;
- be aware of laws and regulations that could affect the security *controls* and *classification* requirements of the *SE's information*; and
- due to the dynamic nature of *information* technology and the need to maintain an adequate level of current knowledge and proficiency in *information security*, a minimum

of twenty two and one half (22.5) hours of Continuing Professional Education (*CPE*) credits must be completed annually. The *CPEs* must be directly related to *information systems* security. The *SE* will provide the opportunity for the *ISO* to earn the required *CPEs* annually.

### **Standard**

- A. The requirement of *CPE* credits help ensure that the *ISO* stays current in this rapidly evolving field and maintain his/her breadth of knowledge. A total of twenty two and one half (22.5) *CPEs* are required annually. *CPEs* must be directly related to *information systems* security.
- B. The annual time period to earn *CPE* credits will coincide with the calendar year (January 1 to December 31). An individual's cycle will begin the January following appointment to the *ISO* Position. Credits must be earned during the current year to qualify and may not be carried forward or backward from year to year.
- C. Approved *Information Systems* (IS) Security Categories include but are not limited to:
  - Access control *systems* & methodology
  - Telecommunications & network security
  - *Security management* practices
  - Applications & *system* development security
  - Cryptology
  - Security architecture and models
  - Operations security
  - Business continuity planning (BCP)
  - Law, investigation and ethics
  - *Physical security*
- D. *CPE* credits are given for related experience outside of normal on-the-job duties. For instance, while time spent independently preparing an *information security* presentation for a community organization would qualify for *CPE* credits, an equivalent amount of time spent on the job preparing a staff presentation, other internal publications or events would NOT qualify.
- E. *CPE* credits are weighted by activity. Below are common categories of activities and the amount of credits earned for each. These activities are not intended to be a complete listing, as many other events such as graduate work in an appropriate academic field, may also qualify. Typically you will earn 1 *CPE* credit for each hour spent engaged in an educational activity. However, some activities are worth more *CPEs*, due to the depth of study or ongoing commitment involved. *CPE* activities include but are not limited to:
  - Earn 1 *CPE* credit for each hour of attendance at a security educational training course or seminar.
  - Earn 1 *CPE* credit for each hour of attendance at a security conference. The New York State Cyber Security Conference qualifies for *CPE* credits.

- Earn 1 *CPE* credit for each hour of attendance at a *State ISO* meeting.
- Earn 1 *CPE* credit for each hour of attendance at a professional security association chapter meeting, such as the International Information Systems Security Certification Consortium (ISC<sup>2</sup>), Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), etc.
- Earn 1 *CPE* credit for each hour of attendance at a higher education academic\_security class. Credit will only be given on passing the course successfully.
- Earn *CPE* credits for preparing courseware, lectures, or training material. The time spent preparing for and delivering each hour of presentation material is valued at 4 *CPE* credits (e.g., a one hour presentation = 4 *CPE*'s, a two hour presentation = 8 *CPE*'s). Preparing for a *State ISO* meeting presentation qualifies. The 4 *CPE*s for each hour of presentation will only be granted for the initial course, lecture or training presentation, thereafter you will receive 1 *CPE* for each hour of presentation.
- Earn *CPE* credits for contributing original work to the Information Systems Security profession. First publication of a security related article will earn the author(s) 10 *CPE* credits. Publication of a security related book will earn 40 *CPE* credits.
- Earn up to 12 *CPE* credits per year, 1 for each month of service on the board of professional security organization, such as ISC<sup>2</sup>, ISSA, ISACA, etc.
- Earn 1 *CPE* for each month of active participation on a *State ISO* workgroup or committee.
- Earn 1 *CPE* credit for each hour of attendance at security webcasts.
- Credits can be earned by completing a self-study program or completing computer-based training and the course provider issues a certificate of completion and supplies the number of *CPE* hours earned for the course. Study material and validated documentation of completion, such as a certificate or diploma, must be retained.
- Reading an *information security* text will be worth 2 *CPE* credits. Credit in this category will be limited to one text per year. If audited, the *ISO* should retain proof of possession, such as the actual book, a sales receipt, invoice, library record, etc.
- Completion and submission of an original *information security* book review to the *State ISOs* will be worth an additional 3 *CPE* credits (limited to one text per year), and will constitute sufficient proof, even in the absence of other proof.
- Earn 1 *CPE* for each hour of attendance at a vendor security product training class or an *information security* specific sales presentation. Credits for a security sales presentation will be limited to 3 per year.

## ***DOCUMENT CHANGE MANAGEMENT***

---

Requests for changes to this *Standard* must be presented by the *SE ISO* to OCS. If the *State ISO* for OCS agrees to the change, he or she will formally draft the change and have it reviewed and approved through the normal OCS approval process. Each *SE ISO* will be responsible for communicating the approved changes to their organization.

This *Standard* will be reviewed at a minimum on an annual basis.

## ***DEFINITIONS & ACRONYMS***

---

Definitions and acronyms for New York State Cyber Security policies, *standards* and *guidelines* can be found in the Definitions and Acronyms document, available at [www.cscic.state.ny.us/lib/policies/](http://www.cscic.state.ny.us/lib/policies/).

## ***CONTACT INFORMATION***

---

Questions concerning this *Standard* may be directed to OCS at (518) 474-0865.