

---

Cyber Security Standard S10-005

**Monitoring System Access and Use**

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>S10-005, V1.1</b>
Standard Title:	<b>Monitoring System Access and Use</b>
Related Policy:	<b>Cyber Security Policy P03-002, Information Security Policy</b>
Replaces & Supersedes:	<b>Cyber Security Standard S10-005, 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**

---

**TABLE OF CONTENTS** ..... 3

**PURPOSE** ..... 4

**SCOPE**..... 4

**STANDARD**..... 5

    PREFACE ..... 5

    MONITORING SYSTEM ACCESS AND USE ..... 5

*Policy*..... 5

*Standard*..... 5

**DOCUMENT CHANGE MANAGEMENT**..... 7

**DEFINITIONS & ACRONYMS** ..... 7

**CONTACT INFORMATION** ..... 7

## **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**.

### Monitoring System Access and Use (P03-002, Part 10. Access Control Policy)

#### Policy

*Systems* and applications must be monitored and analyzed to detect deviation from the access control policy and record events to provide evidence and to reconstruct lost or damaged *data*. Audit logs recording exceptions and other security relevant events must be produced and kept consistent with record retention schedules developed in cooperation with the State Archives and Records Administration (SARA) and *SE* requirements to assist in future investigations and access control monitoring. Audit logs will be created and protected.

#### Standard

Audit logs will include but are not limited to:

A. Successful and unsuccessful *authentication* events to include but not limited to:

- *system* logon/logoff;
- account or user-ID;
- the type of event;
- an indication of success or failure of event;
- the date and time of event; and
- identification of the source of event such as location, IP address, terminal ID or other means of identification.

B. Unsuccessful resource access events to include but not limited to:

- account or user-ID;
- the type of event;
- an indication of the event;
- the date and time of event;
- the resource; and
- identification of the source of event such as location, IP address, terminal ID or other means of identification.

C. Successful and unsuccessful privileged operations including but not limited to:

- use of *system privileged accounts*;
- *system* starts and stops;
- hardware attachments and detachments;
- *system* and network management alerts and errors messages; and
- security events - account/group management and policy changes.

D. Successful and unsuccessful access to log files to include but not limited to:

- account or user-ID;
- the type of event;
- an indication of success or failure of event;
- the date and time of event; and
- identification of the source of event such as location, IP address, terminal ID or other means of identification.

E. Most web servers offer the option to store log files in either the common log format or an extended log format. The extended log format records more *information* than the common log file format. When technically feasible web servers must use extended log format. The extended log format adds valuable logging *information* to your log file so you can determine where messages are coming from, who is sending the message and adds *information* to the log file that would be necessary to trace an attack

## ***DOCUMENT CHANGE MANAGEMENT***

---

Requests for changes to this *Standard* must be presented by the *SE* Information Security Officer (*ISO*) to the New York State Office of Cyber Security (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.