
Cyber Security Standard S10-007

Key Management

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:	S10-007, V1.1
Standard Title:	Key Management
Related Policy:	Cyber Security Policy P03-002, Information Security Policy
Replaces & Supersedes:	Cyber Security Standard S10-007, V1.0, February 12, 2010
Authority:	Section 715 of the Executive Law
Issued By:	Thomas D. Smith, Director, NYS Office of Cyber Security
Original Publication Date:	February 12, 2010
Revision Date:	July 30, 2010

TABLE OF CONTENTS

TABLE OF CONTENTS 3

PURPOSE 4

SCOPE..... 4

STANDARD..... 5

 PREFACE 5

 KEY MANAGEMENT 5

Policy..... 5

Standard..... 5

DOCUMENT CHANGE MANAGEMENT..... 6

DEFINITIONS & ACRONYMS 6

CONTACT INFORMATION 6

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**.

Key Management (P03-002, Part 11. Systems Development and Maintenance Policy)

Policy

A secured environment must be established to protect the *cryptographic keys* used to encrypt and decrypt *information*. Keys must be securely distributed and stored. Access to these keys must be restricted to only those individuals who have a business need to access the keys. Compromise of a *cryptographic key* would cause all *information* encrypted with that key to be considered unencrypted.

Standard

- A. Unencrypted keys must not be stored with the *data* that they encrypt.
- B. Keys will be protected with a password that conforms at a minimum to the User Password Management Standard.
- C. Compromise of a key will require that a new key be generated as soon as possible, once the compromise has been discovered to continue protection of the encrypted *information*.
- D. *Encryption* keys and their associated software products must be maintained for the life of the archived *data* that was encrypted with that product.

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/.

CONTACT INFORMATION

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