

---

Cyber Security Policy P03-002

**Information Security Policy**

Original Publication Date: April 18, 2003  
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 POLICY

Reference:	<b>P03-002, V3.4</b>
Policy Title:	<b>Information Security Policy</b>
Related Standards:	<b>Cyber Security Standard S10-001 through S10-007</b> <b>Cyber Security Policy and Standard PS08-001, Information Classification and Control</b>
Replaces & Supersedes:	<b>Cyber Security Policy P03-002, V3.3, 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>April 18, 2003</b>
Revision Date:	<b>July 30, 2010</b>

# TABLE OF CONTENTS

---

<b>TABLE OF CONTENTS</b> .....	<b>3</b>
<b>PURPOSE</b> .....	<b>5</b>
<b>SCOPE</b> .....	<b>5</b>
<b>POLICY</b> .....	<b>6</b>
PART 1. PREFACE .....	6
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES .....	6
PART 3. INFORMATION POLICY .....	8
<i>Individual Accountability</i> .....	9
<i>Confidentiality / Integrity / Availability</i> .....	9
<i>Policy and Standards Relationship</i> .....	9
PART 4. ORGANIZATIONAL SECURITY POLICY .....	10
<i>Role and Responsibilities of the State Entity Information Security Officer</i> .....	10
PART 5. INFORMATION CLASSIFICATION AND CONTROL POLICY .....	11
PART 6. PERSONNEL SECURITY POLICY .....	12
<i>Including Security in Job Responsibilities</i> .....	12
<i>User Training</i> .....	12
<i>Security Incidents or Malfunctions Management Process</i> .....	13
PART 7. PHYSICAL AND ENVIRONMENTAL SECURITY POLICY .....	14
<i>Physical Security Perimeter</i> .....	14
<i>Equipment Security</i> .....	14
<i>Secure Disposal or Re-use of Storage Media and Equipment</i> .....	14
<i>Clear Screen</i> .....	15
PART 8. COMMUNICATIONS AND NETWORK MANAGEMENT POLICY .....	15
<i>Sharing Information Outside State Entity</i> .....	15
<i>Network Management</i> .....	16
<i>Vulnerability Scanning</i> .....	16
<i>Penetration and Intrusion Testing</i> .....	16
<i>Internet and Electronic Mail Acceptable Use</i> .....	17
<i>External Connections</i> .....	17
<i>Security of Electronic Mail</i> .....	18
<i>Portable Devices</i> .....	19
<i>Telephones and Fax Equipment</i> .....	19
<i>Wireless Networks</i> .....	20
<i>Modem Usage</i> .....	20
<i>Public Websites Content Approval Process</i> .....	20
<i>Electronic Signatures</i> .....	21
<i>Public Key Infrastructure</i> .....	21
PART 9. OPERATIONAL MANAGEMENT POLICY .....	22
<i>Segregation of Security Duties</i> .....	22
<i>Separation of Development, Test and Production Environments</i> .....	22
<i>System Planning and Acceptance</i> .....	23
<i>Protection against Malicious Code</i> .....	23
<i>Software Maintenance</i> .....	23
<i>Information Back-up</i> .....	23
<i>Assessment</i> .....	24
<i>System Security Checking</i> .....	24
PART 10. ACCESS CONTROL POLICY .....	24
<i>User Registration and Management</i> .....	24
<i>Logon Banner</i> .....	25
<i>Privileged Accounts Management</i> .....	25

<i>User Password Management</i> .....	25
<i>Network Access Control</i> .....	26
<i>Remote Access Control</i> .....	26
<i>Segregation of Networks</i> .....	28
<i>Operating System Access Control</i> .....	28
<i>Application Access Control</i> .....	28
<i>Monitoring System Access and Use</i> .....	28
PART 11. SYSTEMS DEVELOPMENT AND MAINTENANCE POLICY .....	29
<i>Input Data Validation</i> .....	29
<i>Control of Internal Processing</i> .....	30
<i>Message Integrity</i> .....	30
<i>Cryptographic Controls</i> .....	30
<i>Key Management</i> .....	30
<i>Protection of System Test Data</i> .....	30
<i>Change Control Procedures</i> .....	31
PART 12. CYBER SECURITY CITIZENS' NOTIFICATION POLICY .....	31
PART 13. COMPLIANCE POLICY .....	33
<i>Monitoring</i> .....	33
<i>Compliance</i> .....	33
<i>Enforcement and Violation Handling</i> .....	33
<b>DOCUMENT CHANGE MANAGEMENT</b> .....	<b>35</b>
<b>DEFINITIONS &amp; ACRONYMS</b> .....	<b>35</b>
<b>CONTACT INFORMATION</b> .....	<b>35</b>

## PURPOSE

---

The events of September 11<sup>th</sup> have forever changed how we view our freedom, and precautions we must take to protect our way of life. There will be and must be much change as we move into this new, uncharted and unforeseen world.

The purpose of this Policy is to define a set of minimum security requirements that all *State Entities (SE)* must meet. This Policy 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 the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this Policy.

The primary objectives of this Information Security Policy and security program are to:

- effectively manage the *risk* of security exposure or compromise within *SE systems*;
- communicate the responsibilities for the protection of *SE information*;
- establish a secure processing base and a stable processing environment;
- reduce, to the extent reasonably possible, the opportunity for errors to be entered into an electronic *system* supporting *SE* business processes;
- preserve management's options in the event of an *information* asset misuse, loss or unauthorized disclosure; and
- promote and increase the awareness of information security in all *SEs*.

## SCOPE

---

This Policy applies to all *SEs*. This Policy is not intended to unilaterally change the terms and conditions of employment. All *SEs*, when coming into compliance with this Policy, must consider all terms and conditions of employment including collective bargaining agreements.

This Policy is applicable to *SEs*, staff and all others, including outsourced *third parties*, which have access to or manage *SE information*. Where conflicts exist between this Policy and a *SE's* policy, the more restrictive policy will take precedence. The Information Security Policy for *SEs* encompasses 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*. This Policy must be communicated to all staff and all others who have access to or manage *SE information*.

## POLICY

---

### Part 1. Preface

This Information Security Policy is 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 this Policy is mandatory. This Information Security Policy sets the direction, gives broad guidance and defines requirements for *information security* related processes and actions across *State Entities (SEs)*. This Policy documents 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*.

### Part 2. Organizational and Functional Responsibilities

- A. **State Entity (SE):** Each *SE* will establish a framework to initiate and control the implementation of *information security* within the *SE*. An Information Security Officer (*ISO*) must be appointed. A process will be established to determine *information sensitivity*, based on best practices, *State* directives, legal and regulatory requirements to determine the appropriate levels of protection for that *information*. The head of each *SE* will ensure that an organization structure is in place for:
- the implementation of information security policies and standards;
  - assigning information security responsibilities;
  - the implementation of a security awareness program;
  - monitoring significant changes in the exposure of information assets to major threats, legal or regulatory requirements;
  - responding to security incidents;
  - the approval of major initiatives to enhance information security;
  - the development of a process to measure compliance with this Policy;
  - the approval of new applications and services; and
  - communicating requirements of this Policy and the associated Information Security Standards to *third parties* and addressing them in *third party* agreements.
- B. **SE Designated Staff:** *SE* designated staff will be responsible for the implementation of this and other *information security* policies and the compliance of *SE* employees to this Policy. The designated staff must educate *SE* employees with regard to *information security* issues. Staff must explain the issues, why the policies have been established, and what role(s) individuals have in safeguarding *information*. Consequences of non-compliance will also be explained.
- C. **Information Owners:** An individual or a group of individuals designated by the *SE* will serve as or represent *information owners* for the *data* and tools they use. *Information*

*owners* are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.). These access privileges must be in accordance with the *user's* job responsibilities. *Information owners* also communicate to the *SE ISO* the legal requirements for access and disclosure of their *data*. *Information owners* must be identified for all *SE information assets* and assigned responsibility for the maintenance of appropriate security measures such as assigning and verifying *information asset classification* and *controls*, managing *user* access to their resources, communicating deficiencies in *controls* to executive management, etc.. Responsibility for implementing security measures may be delegated, though accountability remains with the identified owner of the asset.

- D. **SE Information Security Officer:** The *SE* Information Security Officer has overall responsibility for ensuring the implementation, enhancement, monitoring and enforcement of the *information security* policies and *standards*. The *SE* Information Security Officer is responsible for providing direction and leadership to his or her *SE* through the recommendation of security policies, *standards*, processes and education and awareness programs to ensure that appropriate safeguards are implemented, and to facilitate compliance with those policies, *standards* and processes. The *SE* Information Security Officer is responsible for investigating all alleged *information security* violations. In this role, the *SE* Information Security Officer will follow *SE procedures* for referring the investigation to other investigatory entities, including law enforcement. The *SE* Information Security Officer will coordinate and oversee security program activities and reporting processes in support of this Policy and other security initiatives. For more detail, see Part 4, Organizational Security Policy, Role and Responsibilities of the *SE* Information Security Officer.
- E. **Security Administrators:** When such an individual or individuals exist, the individual or individuals will work closely with the *SE* Information Security Officer and support staff. Security Administrators are the staff normally responsible for administering security tools, reviewing security practices, identifying and analyzing security *threats* and solutions, and responding to security violations. This individual or individuals has administrative responsibility over all user-IDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements. Where a formal *Security Administration* function does not exist, the organization or staff responsible for the *security administration* functions described above will adhere to this Policy.
- F. **Information Technology (IT):** IT management has responsibility for the *data* processing infrastructure and computing network which support the *information owners*. It is the responsibility of IT management to support the Information Security Policy and provide resources needed to enhance and maintain a level of *information security* control consistent with their *SE's* Information Security Policy.

IT management has the following responsibilities in relation to the security of *information*:

- ensuring processes, policies and requirements are identified and implemented relative to security requirements defined by the *SE's* business;

- ensuring the proper controls of information are implemented for which the SE's business have assigned ownership responsibility, based on the SE's classification designations;
  - ensuring the participation of the SE Information Security Officer and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures, and in protecting information assets;
  - ensuring that appropriate security requirements for user access to automated information are defined for files, databases, and physical devices assigned to their areas of responsibility; and
  - ensuring that critical *data* and recovery plans are backed up and kept at a secured off-site storage facility and that recovery of backed-up media will work if and when needed.
- G. **SE Employees:** It is the responsibility of all employees to protect *SE information* and resources, including passwords, and to report suspected security *incidents* to the appropriate manager and the *SE* Information Security Officer.
- H. **Non-SE Employees:** Individuals who work under agreements with the *SE* such as Contractors, Consultants, Vendors, volunteers and other persons in similar positions, to the extent of their present or past access to *SE information*, are also covered by this Information Security Policy.
- I. **Office of Cyber Security (OCS):** OCS is the owner of this Policy and performs as the security consultant to *SE ISOs* and *SEs*. OCS may also perform periodic reviews of *SE* security programs for compliance with this and other security policies and *standards*. OCS establishes and monitors effectiveness of *information security policy, standards* and *controls* within the State of New York.

### Part 3. Information Policy

- A. All *information*, regardless of the form or format, which is created, acquired or used in support of *SE's* business activities, must only, be used for *SE* business. *SE information* is an asset and must be protected from its creation, through its useful life, and to its authorized disposal. It must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. *Information* must be classified and protected based on its importance to business activities, *risks*, and security best practices.
- B. *Information* is among *SEs'* most valuable assets and *SEs* rely upon that *information* to support their business activities. The quality and *availability* of that *information* is key to *SE's* ability to carry out their missions. Therefore, the security of *SE's information*, and of the technologies and *systems* that support it, is the responsibility of everyone concerned. Each authorized *user* of *SE information* has an obligation to preserve and protect *SE information* in a consistent and reliable manner. Security *controls* provide the necessary physical, logical and procedural safeguards to accomplish those goals.
- C. *Information security management* enables *information* to be shared while ensuring protection of that *information* and its associated *information technology equipment* including the network over which the *information* travels. *SE* designated staff is

responsible for ensuring that appropriate physical, logical and procedural *controls* are in place on these assets to preserve the security properties of *confidentiality*, *integrity*, and *availability* of *SE information*.

### Individual Accountability

Individual accountability is the cornerstone of any security program. Without it, there can be no security.

- Access to SE information technology equipment, systems and networks where the information owner has identified the business need for limited user access or information integrity and accountability, must be provided through the use of individually assigned unique identifiers, known as user-IDs, or other technologies including biometrics, token cards, etc.
- Individuals who use SE information technology equipment must only access information assets to which they are authorized.
- Associated with each user-ID is an authentication token, such as a password, which must be used to authenticate the person accessing the *data*, system or network. Information used to authenticate the identity of a person or process must be treated as PPSI and must not be disclosed. This does not include distribution of one-time-use PINs, passwords, or passphrases.
- Each individual is responsible to reasonably protect against unauthorized activities performed under their user-ID.
- For the user's protection, and for the protection of SE resources, user-IDs and passwords (or other tokens or mechanisms used to uniquely identify an individual) must not be shared (refer to Part 10. Access Control Policy, Operating System Access Control, B.).

### Confidentiality / Integrity / Availability

- A. All *SE information* must be protected from *unauthorized access* to help ensure the *information's confidentiality* and maintain its *integrity*. The *information owner* will classify and secure *information* within their jurisdiction based on the *information's value*, *sensitivity* to disclosure, consequences of loss or compromise, and ease of recovery.
- B. Appropriate processes will be defined in the *SE* recovery plan and implemented to ensure the reasonable and timely recovery of all *SE information*, applications, *systems* and security regardless of computing platform, should that *information* become corrupted, destroyed, or unavailable for a defined period (refer to Part 9. Operational Management Policy, Information Backup).

### Policy and Standards Relationship

*SEs* will develop *standards* and *procedures* that support the implementation of this Policy for *systems* and technologies being used within their domains. These security *standards* will be produced and implemented to ensure uniformity of *information* protection and *security management* across the different technologies deployed within an *SE*. The *standards* can be used as a basis for policy compliance measurement.

## Part 4. Organizational Security Policy

Each *SE* must have an information security function led by a Chief Information Security Officer/Information Security Officer (*ISO*).

*Information security* extends well beyond Information Technology (IT). From an enterprise perspective, *information security* is a critical business function that touches all aspects of an organization including programmatic, fiscal, legal, human resources and IT.

Given the critical importance of *information security* and the need to balance *information security* with business drivers, programmatic and technological issues, it is strongly advised that, for *information security* matters, the *ISO* report to a high level executive in the organization who does not have IT operational responsibilities.

The mission of the information security function is to:

- develop, deploy and maintain an information security architecture that will provide security policies, mechanisms, processes, *standards* and *procedures* that meet current and future business needs of the *SE*;
- provide *information security* consulting to the *SE* regarding security threats that could affect the *SE* computing and business operations, and make recommendations to mitigate the *risks* associated with these *threats*;
- assist management in the implementation of security measures that meet the business needs of the individual *SE*;
- develop and implement security training and awareness programs that educate *SE* employees, contractors and vendors with regard to the *SE's information security* requirements;
- investigate and report to management breaches of security *controls*, and implement additional compensating *controls* when necessary to help ensure security safeguards are maintained; and
- participate in the development, implementation and maintenance of disaster recovery processes and techniques to ensure the continuity of the *SE's* business and the security *controls*, in the event of an extended period of computing resource unavailability.

Although *information security* roles and responsibilities may be outsourced to *third parties*, it is the overall responsibility of each *SE* to maintain control of the security of the *information* that it owns.

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

The *SE* Information Security Officer 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 (*CIO*) 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 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.

## Part 5. Information Classification and Control Policy

The following Policy, and its associated Standard, is included in a separate document entitled **Cyber Security Policy and Standard PS08-001, Information Classification and Control**.

*Information* must be properly managed from its creation, through authorized use, to proper disposal. Different kinds of *information* require different levels of protection. This Policy requires that all *information* be classified on an ongoing basis and managed based on its *confidentiality, integrity* and *availability* characteristics.

The *classification* of *information* pursuant to this Policy and application of appropriate *controls* to that *information* do not alter the responsibility of the *SE* to comply with the records retention and disposition requirements of the Arts and Cultural Affairs Law or its responsibility to make records available for public inspection and copying under the provisions of the Freedom of Information Law. The process of classifying *information* pursuant to this Policy may, however, serve as a basis for an *SE* to evaluate the retention and disposition schedules currently in effect for its records and, where appropriate, consider revising those schedules as a means of managing the records that must be protected by the *SE*. Similarly, the *classification* process can facilitate the accurate and efficient application of the exemptions from disclosure enumerated in the Freedom of Information Law by providing a framework for the comprehensive assessment of the *SE's information assets*.

- A. All *information assets* must have an *information owner* established within the *SE's* lines of business. The *information owner* will be responsible for assigning the *information classification*, determining access privileges of *users* or groups of *users* based on job duties, and overseeing daily decisions regarding *information asset* management. Periodic reviews will be performed by the *information owner* to confirm the *classification* of, or reclassify, the *information asset*.

- B. Each *classification* will have an approved set or range of *controls*. If *SE information* is stored by a *third-party*, the *information owner's SE* is responsible for communicating requirements of this Policy and Standard to the *third-party* and addressing them in *third-party* agreements as they relate to the *SE's data*.
- C. An *information asset* must be classified based on the highest level necessitated by its individual *data* elements.
- D. All *Personal, Private, or Sensitive Information (PPSI)* shall be classified with a *confidentiality* of high.
- E. *Merging of information* which creates a new *information asset* or situations that create the potential for *merging* (e.g., backup tape with multiple files) must be evaluated to determine if a new *classification* of the merged *data* is warranted.
- F. If the *SE* is unable to determine the *confidentiality classification* of *information* stored on *electronic storage media*, the *information* must be assumed to have a high *confidentiality classification* and, therefore, is subject to high *confidentiality controls*.
- G. All reproductions of *information* in its entirety must carry the same *confidentiality classification* as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
- H. A written or electronic inventory of all *SE information assets* must be maintained.

## Part 6. Personnel Security Policy

The intent of the Personnel Security Policy is to reduce the *risk* of human error and misuse of *SE information* and facilities to an acceptable level.

### Including Security in Job Responsibilities

Security roles and responsibilities must be documented. These roles and responsibilities will include general responsibilities for all *SE* employees, as well as specific responsibilities for protecting specific *information* and performing tasks related to security *procedures* or processes. Additional security roles and responsibilities for those individuals responsible for *information security* are defined in this document, Part 4 Organizational Security Policy.

### User Training

- A. All individuals with access to *SE information* must receive security awareness training to ensure they are knowledgeable of security *procedures*, their role and responsibilities regarding the protection of *SE information*, and the proper use of *information* processing facilities to minimize security *risks*.
- B. An *information security* awareness program must be developed, implemented and maintained that addresses the security education needs of all *SE* employees. A *SE* security awareness program will be developed by the *SE's* Information Security

Officer to supplement the *SE*'s new employee orientation program, and must be reinforced at least annually.

### **Security Incidents or Malfunctions Management Process**

- A. Formal *incident* or malfunction reporting and response *procedures* must be established, that define the actions to be taken when an *incident* occurs. The following must be included:
- the symptoms of the problem and any messages displayed should be documented;
  - where appropriate, the information technology equipment should be isolated, if possible, and use of it stopped until the problem has been identified and resolved; and
  - the incident must be reported immediately to the appropriate SE manager and the SE ISO.
- B. Feedback mechanisms must be implemented to ensure that individuals reporting *incidents* are notified of the results after the *incident* has been resolved and closed.
- C. An *incident* management process must be established to track the types and volumes of security *incidents* and malfunctions. This *information* will be used by the *SE* to identify recurring or high impact *incidents* and to record lessons learned. This may indicate the need for additional *controls* to limit the frequency, damage and cost of future *incidents*, or to be taken into account in the policy review process.
- D. ***State* employees and contractors must not attempt to prove a suspected weakness unless authorized by the SE ISO to do so.** Testing weaknesses could have unintended consequences.
- E. All *users* of *SE systems* must be made aware of the procedure for reporting security *incidents*, *threats* or malfunctions that may have an impact on the security of *SE information*. All *SE* staff and contractors are required to report any observed or suspected *incidents* to the appropriate manager and the *SE ISO* as quickly as possible.
- F. Approaches to *incident* management must be documented and *procedures* must be clearly identified to ensure responsibilities are defined, resulting in a prompt and organized response to security *incidents*.
- G. *Incident response procedures* must be clearly identified to promote effective response to security *incidents*. Include *procedures* for *information system* failure, *denial of service*, disclosure of *PPSI* and compromised *systems* of software. Once an *incident* has been identified, the following *procedures* must be followed:
- report the action to OCS according to the OCS Incident Reporting Policy P03-001;
  - identify the underlying cause of the *incident* ;
  - identify *procedures* the *SE* will employ to resolve the problem
  - identify *procedures* the *SE* will employ to prevent the same or similar *incident* from occurring;
  - track the response procedure from initial report through follow-up for review and audit purposes; and

- provide adequate follow-up to ensure that individuals involved or affected by the *incident* understand what took place and how the *incident* was resolved.

## Part 7. Physical and Environmental Security Policy

- A. Critical *SE information* processing and storage facilities must be contained in secure areas protected by a defined security perimeter, with appropriate security barriers and some form of access *controls*. Physical protection measures will be implemented to protect the facility from *unauthorized access*, damage and interference.
- B. The *SE* may include *physical security*, such as controlling access to the building, etc. The *SE* will perform periodic *threat* and *risk* analysis to determine where additional *physical security* measures are necessary, and implement these measures to mitigate the *risks*.

### Physical Security Perimeter

- A. Breaching *physical security* can cause a loss of or damage to *SE information*. *Physical security* can be achieved by creating physical barriers around the assets being protected. Each barrier establishes a security perimeter that would require a method of access control to gain entry. This perimeter could be in the form of an entry point with card key access, a staffed reception area, a locked cabinet or office or other physical barrier.
- B. The *SE* will perform a *threat* and *risk assessment* to determine the extent of the perimeter, and types of *controls* necessary to mitigate the *risk*. Based on the *threat* and *risk assessment*, a *physical security* perimeter must be established in *SE* environments where *information* or *information assets* are stored or operational, *SE data* centers, wiring closets for network and telephonic connections, printers where *PPSI* may be printed, and any other location where *information* may be in use or stored. The purpose of the security perimeter is to prevent *unauthorized access* or theft of *information* or *information assets*.

### Equipment Security

*Information technology* equipment must be physically protected from security *threats* and environmental hazards. Protection of *information technology* equipment is necessary to reduce the *risk* of *unauthorized access* to *information* and to protect against loss or damage. Special *controls* may also be necessary to protect supporting facilities such as electrical supply and cabling infrastructure. This protection will include but is not limited to *data* centers, wiring closets, server rooms, and storage facilities where *information technology equipment* and peripherals are stored.

### Secure Disposal or Re-use of Storage Media and Equipment

There is *risk* of disclosure of *PPSI* through careless disposal or re-use of equipment. Formal processes must be established to minimize this *risk*. Storage devices such as hard disk drives and other media (e.g. tape, diskette, CDs, DVDs, cell phones, digital copiers or other devices that store *information*) or paper containing *PPSI* must be physically

destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive *SE information*.

### Clear Screen

To prevent *unauthorized access to information*, automated techniques and *controls* will be implemented to require *authentication* or *re-authentication* after a predetermined period of inactivity for desktops, laptops, *PDA's* and any other *systems* where *authentication* is required. These *controls* may include such techniques as password protected screen savers, automated logoff processes, or *re-authentication* after a set time out period.

## Part 8. Communications and Network Management Policy

- A. All *SE* networks will implement appropriate security *controls* to ensure the *integrity* of the *data* flowing across these networks. If there is a business need, additional measures to ensure the *confidentiality* of the *data* will also be implemented.
- B. The *SE ISO* will ensure that measures are in place to mitigate any new security *risks* created by connecting the *SE* networks to a *third party* network.
- C. Where a *SE* has outsourced a server or application to a *third party* service (such as web applications), the *SE ISO* must perform or have performed periodic security reviews of the outsourced environment to ensure the security and *availability* of the *SE's information* and application.
- D. All connections to the *SE* networks must be authorized by the appropriate Network Manager, and reviewed by the *SE ISO*. Additions or changes to network configurations must also be reviewed and approved through the *SE* Change Management process.

### Sharing Information Outside State Entity

- A. To facilitate the secure sharing of *information*, appropriate security measures must be in place commensurate with the *sensitivity* and *confidentiality* of the *information* being shared. In most cases, the security *confidentiality* requirements of the *data* being shared will determine the level of security required when sharing *data*.
- B. For *information* to be released outside an *SE* or shared between *SEs*, a process must be established that, at a minimum:
  - evaluates and documents the *sensitivity* of the *information* to be released or shared;
  - identifies the responsibilities of each party for protecting the *information*;
  - defines the minimum *controls* required to transmit and use the *information*;
  - records the measures that each party has in place to protect the *information*;
  - defines a method for compliance measurement;
  - provides a signoff procedure for each party to accept responsibilities; and
  - establishes a schedule and procedure for reviewing the *controls*.

## Network Management

All *SEs* must implement a range of network *controls* to maintain security in its trusted, internal network, and ensure the protection of connected services and networks. These *controls* help prevent *unauthorized access* and use of the *SE* private network. The following *controls*, at a minimum must be implemented:

- Operational responsibility for networks will be separate from *information technology* operations when possible;
- Responsibilities and *procedures* for remote use must be established (refer to Part 10. Access Control Policy section of this document);
- When necessary, special *controls* will be implemented to safeguard *data integrity* and *confidentiality* of *data* passing over public networks (*Internet*).

## Vulnerability Scanning

- A. All *SE hosts* that are or will be accessible from outside the *SE* network must be scanned for *vulnerabilities* and weaknesses before being installed on the network, and after software, operating *system* or configuration changes are made. For both internal and external *systems*, scans will be performed at least annually to ensure that no major *vulnerabilities* have been introduced into the environment. The frequency of additional scans will be determined by the *SE ISO* and the *information owner(s)*, depending on the criticality and *sensitivity* of the *information* on the *system*.
- B. Network *vulnerability scanning* will be conducted after new network software or major configuration changes have been made on *systems* that are essential to supporting a process that is critical to a *SE* business, and annually on all other *systems*. The output of the scans will be reviewed in a timely manner by the *SE ISO*, and any *vulnerability* detected will be evaluated for *risk* and mitigated. The tools used to scan for *vulnerabilities* will be updated periodically to ensure that recently discovered *vulnerabilities* are included in any scans.
- C. Where a *SE* has outsourced a server, application or network services to another *SE*, responsibility for *vulnerability scanning* must be coordinated by both *SEs*.
- D. Anyone authorized to perform *vulnerability scanning* must have a process defined, tested and followed at all times to minimize the possibility of disruption. Reports of exposures to vulnerabilities will be forwarded to the *SE ISO* and other defined staff.
- E. Any *vulnerability scanning* other than that performed by OCS must be conducted by individuals who are authorized by the *SE ISO*.

## Penetration and Intrusion Testing

- A. All *SE* computing *systems* that provide *information* through a public network, either directly or through another service that provides *information* externally (such as the *World Wide Web*), will be subjected to *SE* penetration analysis and intrusion testing. Such analysis and testing will be used to determine if:
  - an individual can make an unauthorized change to an application;
  - a *user* may access the application and cause it to perform unauthorized tasks;

- an unauthorized individual may access, destroy or change any *data*; or
  - an unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).
- B. The output of the *penetration testing* and intrusion testing will be reviewed in a timely manner by the *SE ISO*, and any *vulnerability* detected will be evaluated for *risk* and mitigated as appropriate.
- C. The tools used to perform the *penetration testing* will be updated to ensure that recently discovered *vulnerabilities* are included in any testing.
- D. Where a *SE* has outsourced a server, application or network services to another *SE*, *penetration testing* must be coordinated by both *SEs*.
- E. Only individuals authorized by the *SE* will perform *penetration testing*. The *SE ISO* must approve and OCS must be notified 24 hours prior to each *penetration test*. Any other attempts to perform such *penetration testing* will be deemed an *unauthorized access* attempt.

### **Internet and Electronic Mail Acceptable Use**

When *SE* employees connect to the *Internet* using any *SE Internet* address designation or send electronic mail using the *SE* designation, it should be for purposes authorized by *SE* management. The following is not an all-inclusive list, and provides only examples of behavior that could result in security breaches. Specifically, the *Internet* and electronic mail will not be used:

- to represent yourself as someone else (i.e., “*spoofing*”);
- for spamming;
- for unauthorized attempts to break into any computing *system* whether *SE*’s or another organization’s (i.e., hacking);
- for theft or unauthorized copying of electronic files;
- for posting *PPSI* without *authorization* from *SE*;
- for any activity which create a *denial of service*, such as “chain letters”; and
- for “*sniffing*” (i.e., monitoring network traffic), except for those authorized to do so as part of their job responsibilities.

### **External Connections**

(Also see Part 10. Access Control Policy, Remote Access Control)

- A. Because the *Internet* is inherently insecure, access to the *Internet* is prohibited from any device that is connected, wired or wireless to any part of a *SE* network unless specifically authorized by *SE ISO*. This includes accounts with *third party Internet* service providers. *Users* will not use the *SE*’s *Internet* accounts to establish connections to these *third party* services, unless authorized to do so by *SE* management and the security of the connection is reviewed and approved by the *SE ISO*.
- B. All connections from the *SE* network to external networks must be approved in writing by the *SE ISO*. Connections will be allowed only with external networks that

have been reviewed and found to have acceptable security *controls* and *procedures*, or appropriate security measures have been implemented by the *SE* to protect *SE* network resources. A *risk* analysis will be performed to ensure that the connection to the external network will not compromise the *SE*'s private network. Additional *controls*, such as the establishment of *firewalls* and a *DMZ* (demilitarized zone) may be implemented between the *third party* and the *SE*. These connections will be periodically reviewed by the *SE* to ensure:

- the business case for the connection is still valid and the connection is still required; and
  - the security *controls* in place (filters, rules, access control lists, etc.) are current and functioning correctly.
- C. This Policy requires that connection to the *SE* network be done in a secure manner to preserve the *integrity* of the *SE* network, *data* transmitted over that network, and the *availability* of the network. The security requirements for each connection will be assessed individually, and be driven by the business needs of the parties involved. Only *SE* authorized, qualified staff or qualified *third party* will be permitted to use sniffers or similar technology on the network to monitor operational *data* and security events
- D. The *SE ISO* or designee will regularly review audit trails and *system* logs of external network connections for abuses and anomalies.
- E. *Third party* network and/or workstation connection to a *SE* network must have an internal *SE* sponsor develop a business case for the network connection. A *SE* non-disclosure agreement must be signed by a duly appointed representative from the *third party* organization who is legally authorized to sign such an agreement. In addition to the agreement, the *third party*'s equipment must also conform to the *State*'s security policies and *standards*, and be approved for connection by the *SE ISO*.
- F. Any connection between *SE firewalls* over external networks that involves *PPSI* must use *encryption* to ensure the *confidentiality* and *integrity* of the *data* passing over the external network (refer to Cyber Security Standard S10-006, Cryptographic Controls).

### **Security of Electronic Mail**

Electronic mail provides an expedient method of creating and distributing messages both within the organization and outside of the organization. *Users* of the *SE* E-mail *system* are a visible representative of the *State* and must use the *systems* in a legal, professional and responsible manner. Unless prior management approval has been obtained, *SE users* must not connect to commercial E-mail *systems* from any *SE system* or workstation (i.e., AOL, Yahoo, etc.). *Users* of *SE* E-mail *systems* must comply with this Policy and be knowledgeable of their responsibilities as defined in Part 8, Communications and Network Management Policy, Internet and Electronic Mail Acceptable Use.

## Portable Devices

- A. All portable computing resources and *information* media must be secured to prevent compromise of *confidentiality* or *integrity*. No portable device or media may store or transmit *PPSI* without suitable protective measures that are approved by the *SE ISO*.
- B. When using mobile computing facilities such as notebooks, palmtops, laptops and mobile phones, special care must be taken to ensure that *information* is not compromised. Approval is contingent on satisfaction of the requirements for physical protection, access *controls*, *cryptographic* techniques, back-ups, *virus* protection and the rules associated with connecting mobile facilities to networks and guidance on the use of these facilities in public places.
- Care must be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the *SE*'s premises. Protection must be in place to avoid the *unauthorized access* to or disclosure of the *information* stored and processed by these facilities, e.g. using *cryptographic* techniques.
  - It is important that when such facilities are used in public places care must be taken to avoid the *risk* of unauthorized persons viewing *information* on-screen.
  - *Procedures* against malicious software shall be developed and implemented and be kept up to date. Equipment will be available to enable the quick and easy back up of *information*. These back-ups must be given adequate protection against theft or loss of *information*.
  - Equipment containing *PPSI* must be attended at all times or physically secured.
  - Training must be provided to staff using mobile computing resources to raise their awareness on the additional *risks* resulting from this way of working and the *controls* that will be implemented.
  - Employees in the possession of laptops, notebooks, palmtops, and other transportable devices or media must not check these in airline luggage *systems*. These portable devices or media must remain in the possession of the traveler as hand luggage unless other arrangements are required by Federal or *State* authorities.

## Telephones and Fax Equipment

The use of telephones outside the *SE* for business reasons is sometimes necessary, but it can create security exposures. Employees should:

- take care that they are not overheard when discussing *PPSI*.
- avoid use of any wireless or cellular phones when discussing *PPSI*.
- avoid leaving messages containing *PPSI* on voicemail *systems*.
- if sending documents containing *PPSI* via fax, verify the phone number of the destination fax. Contact the recipient to ensure protection of the fax, either by having it picked up quickly or by ensuring that the fax output is in a secure area.
- avoid using *Internet* fax services to send or receive *PPSI*.
- not use *third party* fax services to send or receive *PPSI*.
- not send documents containing *PPSI* via wireless fax devices.
- not send teleconference call-in numbers and passcodes to a pager, if *PPSI* will be discussed during the conference.

- when chairing a teleconference discussing *PPSI*, confirm that all participants are authorized to participate, before starting any discussion.

### **Wireless Networks**

- A. Advances in wireless technology and pervasive devices create opportunities for new and innovative business solutions. However security *risks*, if not addressed correctly, could expose *SE information systems* to a loss of service or compromise of *PPSI*.
- B. Wireless is a shared medium. Everything that is transmitted over the radio waves can be intercepted if the interceptor is within the coverage area of the radio transmitters. This represents a potential security issue in the wireless Local Area Networks (LANs). The security exposure is more evident if the wireless LANs are deployed or used in public areas, such as airports, hotels or conference centers.
- C. No wireless network or wireless access point will be installed without a *risk assessment* being performed and the written approval of the *SE ISO*.
- D. Suitable *controls*, such as *Media Access Control (MAC) address* restriction, *authentication* and *encryption* must be implemented to ensure that a wireless network or access point can not be exploited to disrupt *SE information* services or to gain *unauthorized access* to *SE information*. When selecting wireless technologies, 802.11x wireless network security features on the equipment must be available and implemented from the beginning of the deployment. Refer to Cyber Security Standard S10-006, Cryptographic Controls.
- E. Access to *systems* that hold *PPSI* or the transmission of *PPSI* via a wireless network is not permitted unless appropriate and adequate measures have been implemented and approved by the *SE ISO*. Such measures must include *authentication*, *authorization*, *encryption*, access *controls* and logging (refer to Part 10. Access Control Policy, Monitoring System Access and Use).

### **Modem Usage**

Connecting dial-up modems to *information technology equipment* which is also connected to the *SE*'s local area network or to another internal communication network is prohibited unless the *SE ISO* approves the request, a *risk assessment* is performed and risks are appropriately mitigated.

### **Public Websites Content Approval Process**

- A. The *World Wide Web* provides an opportunity for *SEs* both to disseminate *information* and to provide interactive government services quickly and cost effectively. Because anything posted on a public web server is globally available and each web presence is a potential connection path to *SE* networks, care must be exercised in the deployment of publicly accessible servers. There is also potential for an insecure server to be used or exploited to assist in an unauthorized or illegal activity, such as an attack on another web site.
- B. The content of each public site must be reviewed according to a process that will be defined and approved by the *SE*. A process must be established for reviewing and

approving updates to publicly available content. These reviews must include consideration of *copyright* issues (both the potential publication of *copyright* material and the appropriate protection of *SE copyright* materials), the type of *information* being made available (*confidentiality*, *privacy* and *sensitivity* of the *information*), the accuracy of the *information* and potential legal implications of providing the *information*.

- C. *PPSI* must not be made available through a server that is available to a public network without appropriate safeguards approved by the *SE ISO*. The *SE ISO* will implement safeguards to ensure *user authentication*, *data confidentiality* and *integrity*, access control, *data* protection and logging mechanisms.
- D. The design of a hosting service must be reviewed and approved in writing by the *SE ISO* to ensure that the security of the web server, protection of *SE* networks, performance of the site, *integrity* and *availability* considerations are adequately addressed.
- E. The implementation of any web site or software is subject to all requirements set forth in Part 11, Systems Development and Maintenance Policy. The service must be reviewed and approved by the *SE ISO* to ensure that the collection and processing of *information* meets *SE* security and *privacy* requirements. The review must ensure that the *information* is adequately protected in transit over public and *SE* networks, in storage and while being processed.

### **Electronic Signatures**

New York State's Electronic Signatures and Records Act (ESRA) (9 NYCRR Part 540) provides that the use of an electronic signature that meets the requirements established by ESRA shall have the same validity and affect as a signature affixed by hand. *SEs* must comply with ESRA and any associated rules and regulations.

### **Public Key Infrastructure**

The establishment of Public Key Infrastructure (PKI) based security architecture is a significant undertaking that requires the establishment of the required business processes to support the PKI and the implementation of technology to support the resulting business processes. In order for the *SE* to operate with a PKI based Security Architecture, the following requirements must be satisfied.

- An appropriate trust model must be defined to include all of the stakeholders. The resulting trust domain or multiple trust domains must be supported by the appropriate certificate policies and certification practice statements. These apply to the stakeholders and *users* of *SE systems* and *data*.
- Where PKI is used for digital signatures or *encryption*, it must operate under and comply with the *State* Certificate Policy for Digital Signatures and *Encryption* issued by the Office for Technology and any associated rules and regulations.

## Part 9. Operational Management Policy

- A. All *SE information* processing facilities must have documented operating instructions, management processes and formal *incident* management *procedures* related to *information security* matters, that define roles and responsibilities of affected individuals who operate or use *SE information* processing facilities.
- B. Computing hardware, software or *system* configurations provided by *SE* must not be altered or added to in any way unless exempted by documented written policy, *procedures* or specific written approval of *SE* management.
- C. Where a *SE* provides a server, application or network services to another *SE*, operational and management responsibilities must be coordinated by both *SEs*.

### Segregation of Security Duties

- A. To reduce the *risk* of accidental or deliberate *system* misuse, separation of duties or areas of responsibility must be implemented where practical.
- B. Whenever separation of duties is difficult to achieve, other compensatory *controls* such as monitoring of activities, audit trails and management supervision must be implemented. At a minimum the audit of security must remain independent and segregated from the security function.

### Separation of Development, Test and Production Environments

- A. Separation of the development, test and production environments is required, either logically or physically. Processes must be documented and implemented to govern the transfer of software from the development environment to the production platform. The following *controls* must be considered:
  - development software and tools must be maintained on *systems* isolated from the production environment. Contain development software on physically separate machines or separate them by access controlled domains or directories;
  - access to compilers, editors and other *system* utilities must be removed from production *systems* when not required;
  - logon *procedures* and environmental identification must be sufficiently unique for production testing and development;
  - *Controls* must be in place to issue short-term access to development staff to correct problems with production *systems* allowing only necessary access.
- B. Development and testing can cause serious problems to the production environment if separation of these environments does not exist. The degree of separation between the production and test environments must be considered by each *SE* to ensure adequate protection of the production environment.
- C. Separation must also be implemented between development and test functions. Each *SE* must consider the use of a stable quality assurance environment where *user* acceptance testing can be conducted and changes cannot be made to the programs being tested.

## System Planning and Acceptance

- A. Because *system* and *data availability* is a security concern, advance planning and preparation must be performed to ensure the *availability* of adequate capacity and resources. The security requirements of new *systems* must be established, documented and tested prior to their acceptance and use.
- B. Storage and memory capacity demands must be monitored and future capacity requirements projected to ensure adequate processing and storage capability is available when needed. This *information* will be used to identify and avoid potential bottlenecks that might present a *threat* to *system* security or *user* services.
- C. Acceptance criteria must be developed and documented for new *information systems*, upgrades and new versions of existing *systems*. Acceptance testing will be performed to ensure security requirements are met prior to the *system* being migrated to the production environment. *SE* managers will ensure that the security requirements and criteria for acceptance are clearly defined, agreed, documented and tested.

## Protection against Malicious Code

Software and associated *controls* must be implemented across *SE systems* to prevent and detect the introduction of *malicious code*. The introduction of *malicious code*, such as a *virus*, network *worm* program or *Trojan horse*, can cause serious damage to networks, workstations and business *data*. *Users* must be made aware of the dangers of unauthorized or *malicious code*. *SE* must implement *controls* to detect and prevent a *virus* from being introduced to the *SE* environment. The types of *controls* and frequency of updating signature files, is dependent on the *value* and *sensitivity* of the *information* that could be potentially at *risk*. For most *SE* workstations, *virus* signature files must be updated weekly. On *host systems* or servers, the signature files will be updated daily or when the *virus* software vendor's signature files are updated and published.

## Software Maintenance

- A. All *system* software must be maintained at a vendor-supported level to ensure software accuracy and *integrity*, unless *SE ISO* approves otherwise in writing.
- B. Maintenance of *SE*-developed software will be logged to ensure changes are authorized, tested and accepted by *SE* management.
- C. All known security patches must be reviewed, evaluated and appropriately applied in a timely manner to reduce the *risk* of security *incidents* that could affect the *confidentiality*, *integrity* and *availability* of business *data* or software *integrity*.

## Information Back-up

The scope of this section is limited to the IT infrastructure, and the *data* and applications of the local *SE* environment. A *threat* and *risk assessment* must be performed by the *SE* to determine the criticality of business *systems*, and the time frame required for recovery. To ensure interruptions to normal *SE* business operations are minimized, and critical *SE* business applications and processes are protected from the effects of major failures, each *SE* business unit, including *SE Security Management*, in cooperation with the *SE CIO*,

must develop plans that can meet the IT backup and recovery requirements of the *SE*. Back-ups of critical *SE data* and software must be performed regularly.

### Assessment

An assessment of the criticality of the services provided and the *sensitivity* of the *information* held on all *hosts* and servers (including all installed software and operating *system* versions, *firewalls*, switches, routers and other communication equipment operating *systems*) will be maintained.

### System Security Checking

- A. *Systems* and services that process or store *PPSI* or provide support for critical processes must undergo *technical security reviews* to ensure compliance with implementation *standards* and for vulnerabilities to subsequently discovered *threats*. Reviews of *systems* and services that are essential to supporting a critical *SE* function must be conducted at least once every year. Reviews of a representative sample of all other *systems* and services must be conducted at least once every 24 months.
- B. Any deviations from expected or required results that are detected by the *technical security review* process must be reported to the *SE ISO* and corrected immediately. In addition, the *SE* application owner must be advised of the deviations and must initiate investigation of the deviations (including the review of *system* activity log records if necessary).

## Part 10. Access Control Policy

- A. To preserve the properties of *integrity*, *confidentiality* and *availability*, the *SE*'s *information assets* will be protected by logical and physical access control mechanisms commensurate with the *value*, *sensitivity*, consequences of loss or compromise, legal requirements and ease of recovery of these assets.
- B. *Information owners* are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges will be (read, update, etc.). These access privileges will be granted in accordance with the *user*'s job responsibilities.

### User Registration and Management

- A. A *user* management process shall be established and documented by the *SE* to outline and identify all functions of *user* management, to include the generation, distribution, modification and deletion of *user* accounts for access to resources. The purpose of this process is to ensure that only authorized individuals have access to *SE* applications and *information* and that these *users* only have access to the resources required for authorized purposes.
- B. The *user* management process must include the following sub-processes as appropriate:

- enrolling new *users*;
  - removing user-IDs;
  - granting “privileged accounts” to a user;
  - removing “privileged accounts” from a user;
  - periodic reviewing “*privileged accounts*” of *users*;
  - periodic reviewing of *users* enrolled to any *system*; and
  - assigning a new *authentication* token (e.g. password reset processing).
- C. The appropriate *information owner* or other authorized officer will make requests for the registration and granting of access rights for *State* employees.
- D. For applications that interact with individuals that are not employed by an *SE*, the *information owner* is responsible for ensuring an appropriate *user* management process is implemented. *Standards* for the registration of such external *users* must be defined, to include the credentials that must be provided to prove the *identity* of the *user* requesting registration, validation of the request and the scope of access that may be provided.

### **Logon Banner**

Logon banners must be implemented on all *systems* where that feature exists to inform all *users* that the *system* is for *SE* business or other approved use consistent with *SE* policy, and that *user* activities may be monitored and the *user* should have no expectation of *privacy*. Logon banners are usually presented during the *authentication* process.

### **Privileged Accounts Management**

The issuance and use of *privileged accounts* will be restricted and controlled. Inappropriate use of *system* account privileges is often found to be a major contributing factor to the failure of *systems* that have been breached. Processes must be developed to ensure that uses of *privileged accounts* are monitored, and any suspected misuse of these accounts is promptly investigated. Passwords of *multi-user system privileged accounts* must be changed more often than normal *user* accounts.

### **User Password Management**

- A. Passwords are a common means of authenticating a *user*’s *identity* to access an *information system* or service. Password *standards* must be developed and implemented to ensure all authorized individuals accessing *SE* resources follow proven password management practices. These password rules must be mandated by automated *system controls* whenever possible. These password best practices include but are not limited to:
- passwords must not be stored in clear text;
  - use passwords that are not easily guessed or subject to disclosure through a dictionary attack;
  - keep passwords confidential – do not share individual;
  - change passwords at regular intervals;
  - change temporary passwords at the first logon;

- when technology permits, passwords must contain a mix of alphabetic, numeric, special, and upper/lower case characters; and
  - do not include passwords in any automated logon process, e.g., stored in a macro or function key, web browser or in application code
- B. To ensure good password management, password *standards* must be implemented on all *SE* platforms when technically feasible.

### **Network Access Control**

Access to a *SE*'s trusted internal network must require all authorized *users* to authenticate themselves through use of an individually assigned user-ID and an *authentication* mechanism, e.g., password, token, smart card.... Network *controls* must be developed and implemented that ensure that an authorized *user* can access only those network resources and services necessary to perform their assigned job responsibilities.

### **Remote Access Control**

(Also see Part 8. Communication and Network Management Policy, External Connections)

- A. To maintain *information security*, *SE* requires that individual accountability be maintained at all times, including during *remote access*.
- B. Connection to *SE*'s networks must be done in a secure manner to preserve the *integrity* of the network, *data* transmitted over that network, and the *availability* of the network. Security mechanisms must be in place to control access to *SE systems* and networks remotely from fixed or mobile locations.
- C. Advance approval for any such connection must be obtained from the *SE* management and the *SE ISO*. An assessment must be performed and documented to determine the scope and method of access, the *risks* involved and the contractual, process and technical *controls* required for such connection to take place.
- D. Because of the level of *risk* inherent with *remote access*, use of a stronger password or another comparable method is required prior to connecting to any *SE* network. All sessions are subject to periodic and random monitoring.
- E. When accessing a *SE* network remotely, identification and *authentication* of the entity requesting access must be performed in such a manner as to not disclose the password or other *authentication information* that could be intercepted and used by a *third party*.
- F. Use of a common access point is required. This means that all remote connections must be made through managed central points-of-entry. Using this type of entry *system* to access a *SE* network provides many benefits, including simplified and cost effective security, maintenance, and support.
- G. For a vendor to access *SE systems*, individual accountability is also required. For those *systems* (hardware or software) for which there is a built-in user-ID for periodic maintenance, the account must be disabled until the user-ID is needed. The activity performed while this vendor user-ID is in use must be logged. Since these accounts

are not regularly used, the vendor user-ID must be disabled, the password changed or other *controls* implemented to prevent or monitor unauthorized use of these *privileged accounts* during periods of inactivity.

- H. In the special case where servers, storage devices or other *information technology equipment* has the capability to automatically connect to a vendor to report problems or suspected problems, the *SE ISO* must review any such connection and process to ensure that connectivity does not compromise the *SE* or other *third party* connections.
- I. Working from a remote location must be authorized by *SE* management and appropriate arrangements made for this activity through written policy and procedure, to ensure the work environment at the remote location provides adequate security for *SE data* and computing resources. Appropriate protection mechanisms commensurate with *risk* and exposure must be in place to protect against theft of *SE* equipment, unauthorized disclosure of *SE information*, misuse of *SE* equipment or *unauthorized access* to the *SE* internal network or other facilities by anyone including family and friends. To ensure the proper security *controls* are in place and all *SE* security *standards* are followed, the following must be considered:
- the *physical security* of the remote location including using a laptop at any location other than an employee's work station;
  - the accessing mechanism, given the *sensitivity* of the *SE's* internal *systems* and method of transmitting *information*; and
  - appropriate business continuity *procedures* including backing up critical *information*.
- J. The following *controls* must be considered and appropriately implemented. If/when implemented, they must be monitored and audited:
- a definition of the *classification* of the *information* and the *systems* and services that the remote *user* is authorized to access;
  - documented *procedures* and necessary tools allowing for secure *remote access* such as *authentication* tokens and/or passwords, including *procedures* for revocation of *authorization* and return of equipment;
  - hardware and software support and maintenance *procedures* including anti-*virus* software and maintenance of current signature files;
  - implementation of suitable network boundary *controls* to prevent unauthorized *information* exchange between *SE* networks connected to remote *information technology equipment* and externally connected networks, such as the *Internet*. Such measures include *firewalls* and *intrusion detection* techniques at the remote location; and
  - *physical security* of the equipment used for *remote access* (e.g. such as cable locking device, or locking cabinet/secure storage area).

For *encryption* requirements, refer to Cyber Security Standard S10-006, Cryptographic Controls.

## Segregation of Networks

When the *SE* network is connected to another network, or becomes a segment on a larger network, *controls* must be in place to prevent *users* from other connected networks access to sensitive areas of the *SE*'s private network. Routers or other technologies must be implemented to control access to secured resources on the trusted *SE* network.

## Operating System Access Control

- A. Access to operating *system* code, services and commands must be restricted to only those individuals necessary in the normal performance of their job responsibilities. All individuals (*systems* programmers, database administrators, network and security administrators, etc.) will have a unique *privileged account* (user-ID) for their personal and sole use so that activities can be traced to the responsible person. User-IDs must not give any indication of the *user*'s privilege level, e.g., supervisor, manager, administrator. These individuals should also have a second user-ID when performing normal business transactions, such as when accessing the *SE* E-mail *system*.
- B. In certain circumstances, where there is a clear business requirement or *system* limitation, the use of a shared user-ID/password for a group of *users* or a specific job can be used. Approval by *SE ISO* and *SE* management must be documented in these cases. Additional compensatory *controls* must be implemented to ensure accountability is maintained (refer to Part 3. Information Policy, Individual Accountability)
- C. Where technically feasible, default administrator accounts must be renamed, removed or disabled. The default passwords for these accounts must be changed if the account is retained, even if the account is renamed or disabled.

## Application Access Control

- A. Access to *SE* business and *systems* applications must be restricted to those individuals who have a business need to access those applications or *systems* in the performance of their job responsibilities.
- B. Access to source code for applications and *systems* must be restricted, and these accesses should be further restricted so that authorized *SE* staff and contractors can access only those applications and *systems* they directly support.

## Monitoring System Access and Use

*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.

## Part 11. Systems Development and Maintenance Policy

- A. Software applications are developed or acquired to provide efficient solutions to *SE* business problems. These applications generally store, manipulate, retrieve and display *information* used to conduct *SE* business. The *SE* business units become dependent on these applications, and it is essential the *data* processed by these applications be accurate. It is also critical that the software that performs these activities be protected from *unauthorized access* or tampering.
- B. To ensure that security is built into all *SE information systems*, all security requirements, including the need for rollback arrangements, must be identified during the requirements phase of a project and justified, agreed to and documented as part of the overall business case for an *SE information system*. To ensure this activity is performed, the *SE ISO* must be involved in all phases of the *System* Development Lifecycle from the requirements definition phase, through implementation and eventual application retirement.
- C. Security requirements and *controls* must reflect the business *value* of the *information* involved, and the potential business damage that might result from a failure or absence of security measures. This is especially critical for *Internet* Web and other online applications. The framework for analyzing the security requirements and identifying *controls* to meet them is associated with *threat* assessment and *risk management* which must be performed by the *information owner*, reviewed by the *SE ISO* and written approval by *SE* executive management
- D. A process must be established and implemented for each application to:
- address the *business risks* and develop a profile of the *data* to help to understand the *risks*;
  - identify security measures based on the *risk* profile and protection requirements;
  - identify and implement specific *controls* based on security requirements and technical architecture;
  - implement a method to test the effectiveness of the security *controls*;
  - identify processes and *standards* to support changes, ongoing management and to measure compliance.
- E. *Controls* in *systems* and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level, *SE's System* Development Methodology, and in the *SE's* security *standards* documents. The security measures that are implemented must be based on the *threat* and *risk assessments* of the *information* being processed and cost/benefit analysis.

### Input Data Validation

An application's input *data* must be validated to ensure it is correct and appropriate including the detection of *data* input errors. Personnel must be clearly identified to perform these functions. The checks that are performed on the client side must also be performed at the server to ensure *data integrity*. Checks will be performed on the input of business transactions, static *data* (names, addresses, employee numbers, etc.) and

parameter tables. Set up a process to verify and correct fields, characters, completeness of *data* and range/volume limits.

### **Control of Internal Processing**

*Data* that has been entered correctly can be corrupted by processing errors or through deliberate acts. Checks and balances must be incorporated into *systems* to prevent or stop an incorrect program from running. Application design must ensure that *controls* are implemented to minimize the *risk* of processing failures leading to a loss of *data* or *system integrity*. Consider the use of correction programs to recover from failures and access to add and delete functions to make changes to application *data* and to ensure the correct processing of *data*.

### **Message Integrity**

It is necessary to put into place a method to detect unauthorized changes to the content of a transmitted electronic message. Message *integrity* must be considered for applications where there is a security requirement to protect the message or *data* content e.g. electronic funds transfer, EDI transactions, etc. An assessment of *threats* and *risks* will be performed to determine if message *integrity* is required and to identify the most appropriate method of implementation. It should also be noted that message *integrity* will not protect against unauthorized disclosure.

### **Cryptographic Controls**

- A. *Encryption* is an important security layer that is used to protect the *confidentiality* of *information*. *Encryption* is an effective tool in mitigating the *threat* of *unauthorized access* to *data*. However, there are other *threats*, such as a hacker gaining access to an authorized *user* account or process, where more stringent *controls* and/or the use of multiple *encryption* levels must be considered.
- B. Based on a *risk assessment*, the required level of protection should determine the strength of the *encryption* employed. In deciding what is best for the *SE*, the benefits of both stand-alone and enterprise level *encryption* solutions must be considered. Attention must also be given to the regulations and national restrictions (e.g., export *controls*) that may apply to the use of *cryptographic* techniques in different parts of the world.

### **Key Management**

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.

### **Protection of System Test Data**

- A. Test *data* is intended to test the expected behavior of software, *systems* and applications. Test *data* is developed to test a comprehensive set of conditions and outcomes, including exception processing and error conditions to demonstrate

accurate processing and handling of *information* and the stability of the software, *system* or application.

- B. Once test *data* is developed, it must be protected and controlled for the life of the testing. In those cases where test *data* is reused, whenever modifications are made to the software, *system* or application then the test *data* must be protected and controlled during the entire useful life. This protection mechanism is essential to ensuring a valid and controlled simulation with predictable outcomes.
- C. Production *data* may be used for testing only if the following *controls* are applied:
  - a business case is documented, approved in writing by the *information owner* and access *controls*, *system* configurations and logging requirements for the production *data* are applied to the test environment; or
  - a business case is documented, approved in writing by the *information owner* and *PPSI* will be masked or overwritten with fictional *information* and the *data* will be deleted as soon as the testing is completed.

### Change Control Procedures

- A. To minimize the possibility of corruption of *information systems*, strict *controls* over changes to *information systems* must be implemented. Formal change control *procedures* for business applications must be developed, implemented and enforced. They must ensure that security and control *procedures* are not compromised, that support programmers are given access only to those parts of a *system* necessary to perform their jobs, and that formal agreement and approval processes for changes are implemented. These change control *procedures* will apply to *SE* business applications as well as *systems* software used to maintain operating *systems*, network software, hardware changes, etc.
- B. In addition, access to source code libraries for both *SE* business applications and operating *systems* must be tightly controlled to ensure that only authorized individuals have access to these libraries and that access is logged to ensure all activity can be monitored.

## Part 12. Cyber Security Citizens' Notification Policy

- A. For purposes of this Cyber Security Citizens' Notification Policy, the terms "personal information" and "private information" shall have the meanings prescribed by sections 202 and 208 of the State Technology Law. New York State *values* the protection of private information of individuals. This Policy requires notification to impacted New York residents and non-residents. All *SEs* are required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Breach and Notification Act and this Policy.
- B. The *SE*, after consulting with OCS to determine the scope of the breach and restoration measures, shall notify an individual when it has been determined that there has been, or is reasonably believed to have been a compromise of private information through unauthorized disclosure.

- C. A compromise of private information shall mean the unauthorized acquisition of unencrypted electronic *data* with private information.
- D. If encrypted *data* is compromised along with the corresponding *encryption* key, the *data* shall be considered unencrypted and thus fall under the notification requirements.
- E. Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.
- F. *SE* will notify the affected individual. Such notice shall be directly provided to the affected persons by one of the following methods:
- written notice;
  - electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the *SE* who notifies affected persons in such form;
  - telephone notification provided that a log of each such notification is kept by the *SE* who notifies affected persons; or
  - substitute notice, if a *SE* demonstrates to the *State* Attorney General that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such *SE* does not have sufficient contact *information*. Substitute notice shall consist of all of the following:
    - e-mail notice when such *SE* has an e-mail address for the subject persons;
      - conspicuous posting of the notice on such *SE's* web site page, if such *SE* maintains one; and
      - notification to major Statewide media.
- G. The *SE* shall notify, OCS as to the timing, content and distribution of the notices and approximate number of affected persons.
- H. The *SE* shall notify the Attorney General and the Consumer Protection Board, whenever notification to a New York resident is necessary, as to the timing, content and distribution of the notices and approximate number of affected persons.
- I. Regardless of the method by which notice is provided, such notice shall include contact *information* for the *SE* making the notification and a description of the categories of *information* that were, or are reasonably believed to have been, acquired by a person without valid *authorization*, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.
- J. This Policy also applies to *information* maintained on behalf of a *SE* by a *third party*.
- K. When more than five thousand New York residents are to be notified at one time, then the *SE* shall notify the *consumer reporting agencies* as to the timing, content and

distribution of the notices and the approximate number of affected individuals. This notice, however, will be made without delaying notice to the individuals..

## Part 13. Compliance Policy

### Monitoring

Consistent with applicable law, employee contracts and *SE* policies, the *SE* reserves the right to monitor, inspect, and/or search at any time all *SE information systems*. Since *SE's information technology equipment* and networks are provided for business purposes, staff members shall have no expectation of *privacy* in the *information* stored in or send through these *information systems*. *SE* management additionally retains the right to remove from its *information systems* any unauthorized material.

### Compliance

- A. OCS may periodically review compliance by *State Entities* to this Policy. Such reviews may include, but are not limited to, reviews of the technical and business analyses required to be developed pursuant to this Policy, and other project documentation, technologies or *systems* which are the subject of the published policy or *standard*.
- B. Compliance with this Policy is mandatory. Each *user* must understand his/her role and responsibilities regarding *information security* issues and protecting *SE's information*. The failure to comply with this or any other *security policy* that results in the compromise of *SE information confidentiality, integrity, privacy, and/or availability* may result in appropriate action as permitted by law, rule, regulation or negotiated agreement. Each *SE* will take every step necessary, including legal and administrative measures, to protect its assets and shall establish the post of *SE Information Security Officer* to monitor compliance with policy matters.
- C. At the *State* government entity level, each *SE* shall implement a process to determine the level of compliance with this Policy. A review to ensure compliance with this Policy must be conducted at least annually and *SE Executive Management* will certify and report the *SE's Level of Compliance* with this Policy in writing to the Office of Cyber Security by December 31st of each year. Areas where compliance with the policy requirements is not met will be documented and a plan will be developed to address the deficiencies.
- D. *SE* managers and supervisors will ensure that all security processes and *procedures* within their areas of responsibility are followed. In addition, all business units within the *SE* may be subject to regular reviews to ensure compliance with security policies and *standards*.

### Enforcement and Violation Handling

- A. Any compromise or suspected compromise of this Policy must be reported to the appropriate *SE* management, the *SE Information Security Officer* and OCS as required by this Policy (refer to Part 6. Personnel Security Policy, Security Incident or Malfunctions Management Process). Any violations of security policies may be

subject to disciplinary or other appropriate action in accordance with law, rule, regulation, policy or negotiated agreement.

- B. Security *incident* reports indicating the *risk* level of the violation must be reported to responsible entities in accordance with *SE* labor relations. Access *authorization* for *user* accounts involved in a compromise may be suspended during the time when a suspected violation is under investigation. Automated violation reports generated by the various security *systems* will be forwarded to the appropriate management and the *SE* Information Security Officer for timely resolution.

## ***DOCUMENT CHANGE MANAGEMENT***

---

Requests for changes to this Policy 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 policy approval process. Each *SE ISO* will be responsible for communicating the approved changes to their organization.

This Policy and supporting policies and *standards* 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 Policy may be directed to OCS at (518) 474-0865.