



Cyber Security Policy & Standard
PS08-001

Information Classification and Control

Original Publication Date: October 10, 2008
Revision Date: February 7, 2012

Thomas D. Smith
Director
Office of Cyber Security
New York State Division of
Homeland Security and Emergency Services
State Office Campus, Building 7A
1220 Washington Avenue
Albany, New York 12242



CYBER SECURITY POLICY & STANDARD

Reference:	PS08-001, V1.2
Title:	Information Classification and Control
Related Policy:	Cyber Security Policy P03-002, Information Security Policy
Replaces & Supersedes:	Information Classification and Control, V1.1, December 4, 2008
Authority:	Section 715 of the Executive Law
Issued By:	Thomas D. Smith, Director, NYS Office of Cyber Security
Original Publication Date:	October 10, 2008
Revision Date:	February 7, 2012

TABLE OF CONTENTS

TABLE OF CONTENTS	3
TEMPORARY WAIVER FOR MANDATORY COMPLIANCE	4
PURPOSE	4
SCOPE	4
INFORMATION CLASSIFICATION AND CONTROL	5
PREFACE	5
POLICY.....	5
STANDARD.....	7
EXCEPTION PROCESS	10
DOCUMENT CHANGE MANAGEMENT	10
DEFINITIONS & ACRONYMS	10
CONTACT INFORMATION	10
APPENDICES	
APPENDIX A. EXCEPTION REQUEST FORM	
APPENDIX B. INFORMATION CLASSIFICATION MANUAL	
APPENDIX C. INFORMATION ASSET CLASSIFICATION WORKSHEET	
APPENDIX D. INFORMATION CONTROL CHARTS	
APPENDIX E. GLOSSARY OF INFORMATION SECURITY CONTROLS	

TEMPORARY WAIVER FOR MANDATORY COMPLIANCE

Recognizing that current economic conditions within our State have placed competing demands on limited resources, this Policy and Standard has been reissued as a best practice guideline. The initial compliance deadline has been suspended, however, it is anticipated that this Standard will become mandatory at a later date. In the interim, we are asking Agencies to adopt this Standard as best practice and proceed with implementation as resources allow.

Many of the requirements set forth in the Standard can be accomplished without expenditure and will assist your Agency in fulfilling its obligation to protect the information that New York State citizens have entrusted to our care.

PURPOSE

The purpose of this Policy and Standard is to define a *classification* scheme for *information*, provide *procedures* for classifying *information*, and supply baseline *controls* to protect the *confidentiality*, *integrity* and *availability* of *information*. This Policy and Standard shall serve as best practices for the State University of New York and the City University of New York campuses. Any *State Entity (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 and Standard.

The primary objective of the **Information Classification and Control Policy and Standard** is to uniformly protect *information* entrusted to New York State entities.

SCOPE

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

This Policy and Standard is applicable to *State Entities*, staff and all others, including outsourced *third parties*, which have access to or manage *SE information*. Where conflicts exist between this Policy or Standard and a *SE's* policy or *standard*, the more restrictive policy or *standard* will take precedence. The scope of this Policy and Standard includes *information* through its entire life cycle (i.e., generation, use, storage and disposition). It covers *information* in any form including electronic, paper, voice, video or other physical forms. This Policy and Standard must be communicated to all staff and all others who have access to or manage *SE information*.

INFORMATION CLASSIFICATION AND CONTROL

Preface

This document includes both the **Information Classification and Control Policy** and the **Information Classification and Control Standard**. The Policy is part of the broader **Information Security Policy** (P03-002) and is included in this document for ease of reference.

In order to facilitate the process of classifying *information assets* an **Information Classification Manual**, **Information Asset Classification Worksheet**, **Information Control Charts** and **Glossary of Information Security Controls** are provided in the Appendices. The Information Classification Manual, in conjunction with the Worksheet provides a process for classifying *information assets* and contains the minimum mandatory questions that must be answered when classifying *information*. The Control Charts contain the mandatory baseline *controls* that must be implemented based on the *information classification*. The Glossary contains explanations for each control. A *SE* may add more questions and/or *controls* but may not alter or remove the original questions and *controls*.

Please note the Worksheet and the Control Charts and Glossary are available in an automated tool called the Information Asset Classification System (IACS). This application is available to all New York State governmental entities utilizing NYS Directory Services. For further information, contact the Office of Cyber Security (OCS) at (518) 242-5200 or ocs.info@dhses.ny.gov.

The terms *data* and *information* will be used interchangeably throughout this document.

Policy

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 a *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.

Standard

- A. *Information classification* is based on three *principles* of security: 1) *confidentiality*, 2) *integrity*, and 3) *availability*. For each *principle*, *information* can be classified as low, moderate, or high based on the potential impact. Impact levels are defined as minimal, limited and severe. For purposes of *classification*, minimal impact shall be deemed to include no impact.

Minimal impact would:

- cause a degradation in mission capability to an extent and duration that the *SE* is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- result in minor damage to *SE* or *third party* assets;
- result in minor financial loss; or
- result in minor harm to individuals.

Limited impact would:

- cause a significant degradation in mission capability to an extent and duration that the *SE* is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- result in significant damage to *SE* or *third party* assets;
- result in significant financial loss; or
- result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Severe impact would:

- cause a degradation in or loss of mission capability to an extent and duration that the *SE* is not able to perform one or more of its primary functions;
- result in major damage to *SE* or *third party* assets;
- result in major financial loss; or
- result in catastrophic harm to individuals involving loss of life or serious life threatening injuries.

You can refer to Section 2.2 of the Information Classification Manual, Information Asset Classification Questions (Appendix B), for impact level examples.

Each *SE* should review the impact levels in the context of its own operational environment. Figure 1 shows the Information Asset Classification Matrix.

	INFORMATION CLASSIFICATION CATEGORIES		
	LOW	MODERATE	HIGH
<p>CONFIDENTIALITY Consider impact of unauthorized disclosure on factors such as:</p> <ul style="list-style-type: none"> • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust 	The unauthorized access or disclosure of information would have <i>minimal or no impact</i> to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of information would have only <i>limited impact</i> to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of PPSI or other information would have a <i>severe impact</i> on the organization, its critical functions, workforce, business partners and/or its customers.
<p>INTEGRITY Consider impact of unauthorized modification or destruction on factors such as:</p> <ul style="list-style-type: none"> • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust 	The unauthorized modification or destruction of information would have <i>minimal or no impact</i> to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have only <i>limited impact</i> to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have a <i>severe impact</i> on the organization, its critical functions, workforce, business partners and/or its customers.
<p>AVAILABILITY Consider impact of untimely or unreliable access to information on factors such as:</p> <ul style="list-style-type: none"> • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust 	The disruption of access to or use of information would have <i>minimal or no impact</i> to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have only <i>limited impact</i> to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have a <i>severe impact</i> on the organization, its critical functions, workforce, business partners and/or its customers.

Figure 1: Information Asset Classification Matrix

(Based on the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199 – Standards for Security Categorization of Federal Information and Information Systems)

- B. The Information Control Charts correspond to the levels (i.e., low, moderate, high) for each of the security principles (i.e., *confidentiality*, *integrity* and *availability*). Each chart identifies mandatory baseline *controls*, unless otherwise noted.
- C. The *SE* has a responsibility to protect the *confidentiality*, *integrity* and *availability* of *information* generated, accessed, modified, transmitted, transported, stored, or disposed thereof, irrespective of the medium on which the *information* resides and regardless of format.
- D. Protecting *information* is a shared responsibility. Each person may have more than one role and several people may act in the same role. In such cases where the responsibility is divided among multiple individuals or groups, there should be a clear delineation of responsibilities.

For the purposes of *information classification*, the applicable roles as defined in the Information Security Policy (P03-002) are summarized below:

State Entity (SE):

- implement managerial, operational, physical and technical *controls* to comply with the Information Security Policy (P03-002) and this Policy and Standard;
- communicate *controls* to the *SE workforce* and *third parties*;
- employ concept of *least privilege* or *role-based access control* for determining access rights;
- require *SE workforce* compliance;
- address compliance in *third party* agreements;
- maintain a written or electronic inventory of *SE information assets*; and
- identify a central unit responsible to review the *classification* levels assigned by the *information owner* to ensure consistency throughout the organization.

Information Owner:

- assign *classification* levels to *information*, based on the highest level necessitated by its individual *data* elements, on an ongoing basis;
- verify that the *information* resources they have been assigned responsibility for are adequately protected based on the *classification* and corresponding control chart;
- communicate deficiencies in *controls* to executive management;
- determine who is allowed access to the *information* and the type of access;
- communicate to the *SE ISO* the legal requirements for access and disclosure of their *information*; and
- create a plan to periodically review the *classification* level of the *information* based on new *risks*, laws and regulations.

Information Custodian:

- oversee the implementation of safeguards to protect and control access to the *information* based on the *classification*; and
- implement *controls* (authorized by the *information owner's SE*) to comply with the Information Security Policy (P03-002) and this Policy and Standard.

SE Workforce:

- follow guidelines/policies/*procedures* provided by the *SE* for *information* generation, use, storage and disposal;
- exercise appropriate care in protecting *information* in their possession from *unauthorized access*, alteration, destruction or improper use;
- report suspected or actual violations of policies and *standards*; and
- report suspected or actual security breaches or compromises to appropriate *SE* management and the *SE ISO*.

Information Security Officer (ISO):

- advise and assist *information owners* in determining *classifications*; and
- periodically review requirements for *information* protection.

Exception Process

In limited situations an *SE* may determine that a particular control can not be implemented due to technical constraints, business limitations or statutory requirements. The *SE* may mitigate the *risk* associated with not implementing that *control* through the use of *compensating controls*. The decision to mitigate *risk* requires documentation which must include an understanding of the *risk* and a list of *compensating controls*. Only *SEs* that have undertaken a *risk* analysis and have legitimate technological or business constraints can consider the use of *compensating controls*.

The *SE* must complete an **Information Classification and Control Standard Exception Request** form (Appendix A) signed by the *SE ISO*, *CIO*, and Commissioner/Executive Deputy Commissioner, or equivalent. This document must be submitted to the Office of Cyber Security (OCS) for review. Exception requests are valid for a period of one year. After this time the control must be reevaluated. If the control still can not be implemented, a new exception request form must be completed and submitted to OCS.

DOCUMENT CHANGE MANAGEMENT

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

This Policy and 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.dhses.ny.gov/ocs/resources/.

CONTACT INFORMATION

Questions concerning this Policy and Standard may be directed to the New York State Office of Cyber Security (OCS) at (518) 242-5200.

Information Classification and Control Appendix A

Exception Request Form

Original Publication Date: October 10, 2008
Revision Date: February 7, 2012



NEW YORK STATE
OFFICE OF CYBER SECURITY

**Information Classification and Control Standard
Exception Request**

Section 1: Exception Description		
1.1 Requestor Information		
Name:	Phone:	Date:
Agency/Division:	E-mail:	
1.2 Exception Details		
Control Number:		
Control Name:		
Exception Review Date (re-authorization will be required minimally once a year):		
System(s)/ Hardware Impacted:	Will this impact the processing/ storage/ transmission of PPSI?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.3 Reason for Exception Request: List constraints precluding compliance with the control		
1.4 Description of Risk(s): Identify risk(s) posed by the lack of the original control		
1.5 Compensating Control(s): List the compensating control(s) and explain how they address the objectives of the original control		
1.6 Information Owner/Business Manager	Name/Signature:	Date:

Section 2: Executive Authorization		
2.1 Information Security Officer	Name/Signature:	Date:
2.2 Chief Information Officer	Name/Signature:	Date:
2.3 Commissioner/Executive Deputy Commissioner or equivalent	Name/Signature:	Date:

Please mail to State Office Campus, Bldg 7A, 1220 Washington Avenue, Albany, NY 12242 or fax to (518) 322-4976.

Information Classification and Control Appendix B

Information Classification Manual

Original Publication Date: October 10, 2008
Revision Date: February 7, 2012

INFORMATION CLASSIFICATION MANUAL

Preface

Please note the materials described in this Manual (i.e., the Information Asset Classification Worksheet, the Information Control Charts, and the Glossary of Information Security Controls) are available in an automated tool called the Information Asset Classification System (IACS). This application is available to all New York State governmental entities utilizing NYS Directory Services. For further information, contact the Office of Cyber Security (OCS) at (518) 242-5200 or ocs.info@dhses.ny.gov.

Audience

The audience for this Manual is State Entity (SE) executive management and SE information owners. SE executive management is responsible for implementing managerial, operational, physical and technical controls to comply with the Information Classification and Control Policy and Standard. Information owners are responsible for making classification and control decisions regarding the use of information. See Part 2 of Information Security Policy P03-002, Organizational and Functional Responsibilities.

Introduction

The classification of information will be the basis for many information security decisions in an organization. Before deciding the level of resources (i.e., money, time, and technology) required for protection, it is essential that you know what information needs to be protected and the level of protection that is required. The purpose of this Manual is to provide a framework for inventorying and classifying information.

The information classification process will include the following steps:

1. Identify information assets.
2. Classify information assets by confidentiality, integrity, and availability (CIA) through the use of guided questions and examples.
3. Determine controls using the appropriate classification based control chart.

1. Identification of Information Assets

Identification of information assets involves creating an inventory of all information assets in the State Entity (SE). The following items need to be considered when constructing this inventory:

- Grouping of information assets
- Determining the information owner
- Determining the information custodian
- Identifying information assets

1.1 Grouping of Information Assets

In order to facilitate the classification of information assets and allow for a more efficient application of controls, it may be desirable to group information assets together. It is

important to establish that the grouping of assets for classification is appropriate. A broad grouping may result in applying controls unnecessarily as the information asset must be classified at the highest level necessitated by its individual data elements. For example, if a Human Resources unit decides to classify all of their personnel files as a single information asset and any one of those files contains a name and social security number, the entire grouping would need to be protected with the controls for a confidentiality of high.

A narrow grouping allows for more precise targeting of controls. However, as there are more information assets to classify, this increases the complexity of the classification and the management of controls. Using the previous example, classifying the multitude of personnel files (e.g., appointment letters, timecards, position classifications, holiday waivers) as individual information assets requires a different set of controls for each classification.

In the case of a system (e.g., database, data warehouse, application server), it may be easier to apply controls if the system is classified as a single entity. However, costs may be reduced by applying the controls to the individual elements (e.g., field, record, application). Therefore, it is important that the SE evaluate the difference between the two to identify the most appropriate solution when determining the grouping of information assets for classification.

1.2 Determining the Information Owner

It is important to place the responsibility for the classification and control of an information asset with an individual/position. This should be an individual in a managerial position. If multiple individuals are found to be “owners” of the same information asset, an individual owner should be designated by a higher level of management. The information owner is responsible for determining the information’s classification and how and by whom the information will be used.

1.3 Determining the Information Custodian

Information custodians are people, units, or organizations responsible for implementing the authorized controls for information assets based on the classification level. Based on the information owner’s requirements, the custodian is able to take the necessary actions to secure the information, applying safeguards appropriate to the information’s classification level. Information custodians are expected to have a general knowledge of information security in order to skillfully deploy appropriate controls. Information custodians can be from within the SE (e.g., the IT unit) or from third parties (e.g., another SE or non-State entity). If the custodian is a third party, a formal, written agreement between the custodian’s organization and the SE that owns the information should specify the responsibilities of each.

1.4 Identifying Information Assets

An efficient approach towards identifying information assets is for the SE to request that each information owner complete a worksheet for each information asset in their control. The worksheet should minimally include the following:

1. Source of the information asset (e.g., unit, agency)
2. Use of the information asset (i.e., purpose/business function)
3. Business processes dependent on the information asset

4. Users/groups of users of the information asset
5. Owner of the information asset

Information assets can be identified using the template provided (Figure 1/Figure 2) or this information can be extracted from an existing information inventory, if available. Job titles, in place of named individuals, can be used for the custodian, owner and users in order to ease maintenance of your information asset inventory. This template is part of the **Information Asset Classification Worksheet** (Appendix C) which has been provided for your use in classifying information.

Information Asset Identification	
Completed By:	Peter Pasquale, Assistant Director, Finance Unit
Completed Date:	10/10/2008
Department:	Finance
Name of Information Asset:	Purchase Requisition
Information Asset Description/Comment:	Purchase Requisition
Information Asset Use:	Track purchases
Information Asset Format:	Electronic
Information Asset Storage:	Financial Management System Database
Source of Information:	Requisition and Order Processing Unit
Business Process(es) Supported:	Budget/Finance
Information Owner:	Peter Pasquale
Information Custodian:	Financial Management System Database Administrator
Internal Information User(s):	Finance Unit
External Information User(s):	None
Information Asset ID Number:	500

Figure 1: Information Asset Identification Template by Single Asset

Information Asset Identification	
Completed By:	Peter Pasquale, Assistant Director, Finance Unit
Completed Date:	10/10/2008
Department:	Finance
Name of Information Asset:	Purchase Records Group
Information Asset Description/Comment:	Consists of Purchase Request, Purchase Quote, Purchase Requisition, Invoice, Payment Approval
Information Asset Use:	Track purchases
Information Asset Format:	Electronic, Paper
Information Asset Storage:	Financial Management System Database, Finance File Cabinet
Source of Information:	Requisition and Order Processing Unit
Business Process(es) Supported:	Budget/Finance
Information Owner:	Peter Pasquale
Information Custodian:	Financial Management System Database Administrator, Finance Unit
Internal Information User(s):	Finance Unit
External Information User(s):	None
Information Asset ID Number:	501

Figure 2: Information Asset Identification Template by Grouped Asset

2. Classification of Information Assets

Classification of information assets is facilitated by the use of a series of questions. The answers will help determine the information asset classification. Examples are provided to facilitate this process.

2.1 Information Needed for Determining the Classification

To answer the questions effectively, the information owner may recruit and work with subject matter experts who have specific knowledge about the information asset, such as Counsel’s Office and the Records Management Officer. The SE Information Security Officer (ISO) may also be called upon to advise and assist the information owner in determining the classification.

Before starting on the **Information Asset Classification Worksheet**, it may be beneficial for the information owner to familiarize themselves with the following areas. This information will prepare the information owner for filling out the **Information Asset Classification Worksheet**.

Source, Purpose and Value:

- How the information asset is used in supporting business functions.
- How often the information asset is used.
- How often the information asset is updated.
- Dependencies between this information asset and others.
- The cost of creating and duplicating the information.

Legal Requirements:

- Laws, regulations, policies, or contracts that mandate special security requirements for the information (e.g., Health Information Portability and Accountability Act (HIPAA)).
- Retention requirements for the information asset.

Access Requirements:

- Who has/should have access to the information (i.e., people, positions, organizational units).
- Whether the information is shared among other units/SEs, third-parties, Federal/local governments.

Health and Safety Concerns:

- Impact on SE employees, as well as, the public.

Mission:

- The overall mission of the SE.
- The information owner's role (or unit's role) in completing the mission.

Non-tangible Effects:

- Impact if information asset is not available (temporarily or permanently).
- The effect of a breach of confidentiality, integrity, or availability on the non-tangible assets of the SE such as reputation, trust and morale.

2.2 Information Asset Classification Questions

An information asset is classified by confidentiality, integrity, and availability. Each of these three principles of security is individually rated as low, moderate, or high. For example, an information asset may have a confidentiality level of "high", an integrity level of "moderate", and an availability level of "low". The Information Asset Classification Matrix (Figure 3) demonstrates the rationale for making these categorizations at a very general level. The determination of impact severity is subjective.

	INFORMATION CLASSIFICATION CATEGORIES		
	LOW	MODERATE	HIGH
<p>CONFIDENTIALITY Consider impact of unauthorized disclosure on factors such as:</p> <ul style="list-style-type: none"> • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust 	<p>The unauthorized access or disclosure of information would have minimal or no impact to the organization, its critical functions, workforce business partners and/or its customers.</p>	<p>The unauthorized access or disclosure of information would have only limited impact to the organization, its critical functions, workforce, business partners and/or its customers.</p>	<p>The unauthorized access or disclosure of Personal, Private, or Sensitive Information (PPSI) or other information would have a severe impact on the organization, its critical functions, workforce, business partners and/or its customers.</p>
<p>INTEGRITY Consider impact of unauthorized modification or destruction on factors such as:</p> <ul style="list-style-type: none"> • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust 	<p>The unauthorized modification or destruction of information would have minimal or no impact to the organization, its critical functions, workforce, business partners and/or its customers.</p>	<p>The unauthorized modification or destruction of information would have only limited impact to the organization, its critical functions, workforce, business partners and/or its customers.</p>	<p>The unauthorized modification or destruction of information would have a severe impact on the organization, its critical functions, workforce, business partners and/or its customers.</p>
<p>AVAILABILITY Consider impact of untimely or unreliable access to information on factors such as:</p> <ul style="list-style-type: none"> • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust 	<p>The disruption of access to or use of information would have minimal or no impact to the organization, its critical functions, workforce, business partners and/or its customers.</p>	<p>The disruption of access to or use of information would have only limited impact to the organization, its critical functions, workforce, business partners and/or its customers.</p>	<p>The disruption of access to or use of information would have a severe impact on the organization, its critical functions, workforce, business partners and/or its customers.</p>

Figure 3: Information Asset Classification Matrix
(Based on the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199 – Standards for Security Categorization of Federal Information and Information Systems)

A set of questions has been developed to help determine classification ratings. These questions are categorized by confidentiality, integrity, and availability. If it is determined after answering a question that the rating for a security principle (e.g., confidentiality) is high, you are not required to complete the remaining questions in that category. However,

doing so may provide you with a better understanding of the risks associated with the information asset. To save time, the questions at the beginning will typically help in determining whether the rating is high. Each question must be answered sequentially, to the best of the information owners' abilities.

The **Information Asset Classification Worksheet** (Appendix C) contains the minimum questions that must be answered when classifying information. A SE may add more questions but may not alter or remove the original questions. The questions, with examples, are provided below for your reference.

Confidentiality Questions

[1] Does the information include or contain PPSI (Personal, Private or Sensitive Information)?

Example(s): A W-2 form contains a name, as well as a social security number. This would be considered private information and therefore have a confidentiality of high. See the Definitions and Acronyms document available at www.dhses.ny.gov/ocs/resources/ for a definition of PPSI.

[2] What impact does unauthorized access or disclosure of information have on health and safety?

Example(s): There may be information which, if publicly released, may impact the health and safety of the SE's workforce and NYS citizens. For instance, the blueprint and drawings of critical infrastructure buildings, critical infrastructure related systems and network configurations, and disaster recovery/business continuity plans could be exploited by criminals to sabotage or destroy buildings, emergency services, and critical infrastructure operations resulting in a severe impact thereby placing these items in the high confidentiality category.

[3] What is the financial impact of unauthorized access or disclosure of information?

Example(s): The SE may be exposed to litigation or regulatory fines due to disclosure of information protected by confidentiality agreements. For instance, unauthorized release of vendor bid information before the final submission date could jeopardize the bidding process leading to litigation.

Similarly, if the investment decisions of a retirement system become known prior to their execution, it could alter the market sentiment ahead of the investment causing financial losses.

[4] What impact does unauthorized access or disclosure of information have on the SE mission?

Example(s): An agency may be charged with ensuring that illegal goods do not enter State borders. As part of that mission, the agency may be responsible for collecting information regarding unmanned border crossings. If there was an unauthorized release of that information, resulting in an increase of illegal traffic across State borders, it could have a severe impact on the agency's ability to conduct its mission.

An example of minimal impact would be the release of employee contact information which may result in additional phone calls/emails/office visits.

If a list of local delivery restaurants and their phone numbers is disclosed, there would be no impact.

[5] What impact does unauthorized access or disclosure of information have on the public trust?

Example(s): It is important for the government to maintain the public's trust. Any breach of confidentiality that violates the public trust would typically lead to a severe impact for the SE. For example, the exposure of confidential medical records via a security breach could lead to a loss of public trust.

A department which collects and maintains the confidential records of citizens requires a high level of trust from the public. Disclosure of data through a malicious insider, external hacker, or through a random accident could erode trust leading to political consequences for department management and for the State as a whole.

[6] Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or disclosure of information.

Example(s): Some types of information, including personal health records, student grades, and financial and personnel records may be protected by Federal, State, and local laws. Disclosing this information can lead to civil or criminal liability. There are several key statutes, such as HIPAA, that should be examined based on the information asset being classified.

[7] Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure of information.

Example(s): Some information generated within a SE is for internal use only and is not meant to be disclosed externally. The confidentiality of such information varies considerably based on the information asset. Information, such as system security configurations, which, if released, could jeopardize the security of a SE's assets, would require high confidentiality controls.

Administrative information, such as procedures for travel approval, though not publicized outside the SE, would be information that the public could legitimately obtain and should be ranked as low in confidentiality.

[8] Is the information publicly available?

Example(s): Information that must be lawfully made available to the general public from Federal, State, or local government records or any information that does not need to be withheld for security or privacy concerns is generally public. Examples include public transportation schedules, a listing of local city events and health improvement guidelines. These items would be ranked low in confidentiality.

Integrity Questions

[1] Does the information include medical records?

Example(s): In the case of a health care institution, it is important that medical records and medical history are accurate. For example, it may be important to know whether someone is allergic to specific medications so that they are not administered. In addition, it would be necessary to know whether a person has a particular illness or medical condition which would require special treatment. Malicious alteration to such records in medical institutions can cause serious health consequences for the patients. Medical records require high integrity.

[2] Is the information (e.g., security logs) relied upon to make critical security decisions?

Example(s): It is important that security records (e.g., computer security logs, building security access logs) are accurate in order to verify legitimate access and identify unauthorized access attempts. Security records require high integrity.

[3] What impact does unauthorized modification or destruction of information have on health and safety?

Example(s): There is a potential for severe impact on the safety of citizens if someone accesses an airline system and modifies the onboard navigation system.

The removal or editing of surveillance tapes may have a limited or severe impact depending on the presence of other information provided by surveillance.

Something that could be of minimal to no impact on health and safety would be the modification of employee calendars.

[4] What is the financial impact of unauthorized modification or destruction of information?

Example(s): There are many financial implications for the destruction or modification of information. It does not strictly mean monetary loss, but can also indicate loss of employee time and effort for recovery. Something that would have severe financial impact might be the loss of all financial records from a SE's financial management database.

If a database of vendor contact information was deleted, it would involve effort in re-creating the database. This would probably be of minimal impact.

[5] What impact does the unauthorized modification or destruction of information have on the SE mission?

Example(s): SE operations could be drastically affected if information is changed without authorization. For example, if someone removed all the phone numbers in a Do Not Call registry, it would severely impact the mission of the program to prevent unwanted calls to registered numbers.

The mission of a university is to provide education and certify the qualifications of students through academic degrees. Malicious or accidental changes to student academic records would have a severe impact on the university's mission of issuing academic credentials.

[6] What impact does unauthorized modification or destruction of information have on the public trust?

Example(s): The public relies on government to provide accurate information. Failure to do so would erode public trust. For example, if information on certification for licensed professionals was inaccurately modified without authorization and then posted to a public web site, the public would no longer trust the posting SE as a reputable source for this information.

[7] Is integrity addressed by law or regulation? If yes, determine the impact of unauthorized modification or destruction of information.

Example(s): Some types of information, including personal health records, student grades, and financial and personnel records, may be protected by Federal, State, and local laws. Allowing unauthorized changes to information may have legal consequences. There are several key statutes that should be examined based on the information asset being classified. For example, HIPAA requires safeguards to protect against threats to the integrity of electronic protected information.

[8] Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, determine the impact of unauthorized modification or destruction of information.

Example(s): It is important for financial information to remain reliable. Unauthorized changes to financial transactions (e.g., direct deposit, electronic funds transfer) could severely impact the financial stability of a SE.

Employee appraisal records are used to make important personnel decisions. Someone may attempt to falsify records in hopes of getting a promotion, alternate employment or to diminish someone else's reputation and/or record. The impact to the SE could vary dependent upon the situation.

Availability Questions

[1] Is availability of the information essential for emergency response or disaster recovery?

Example(s): If the information asset is required for emergency response, it could be essential in saving lives or in coordinating law enforcement and health officials during an emergency or disaster. Therefore, it must be available upon immediate request (high availability).

Disaster Recovery Plans need to be available in case of emergencies. Although required infrequently, they have a high availability status.

[2] This information needs to be provided or available:

As time permits

Within 1 to 7 days

24 hrs. per day/7 days a week

Example(s): Intrusion detection systems send event notifications so that an incident can be analyzed and escalated based on the level of threat. Since security is critical, and severe damage can be caused to SE data and networks, this operation is time critical and requires high availability.

[3] What is the impact to health and safety if information were not available when needed?

Example(s): Medical records contain information (e.g., allergies, blood type, previous medications) which is critical for providing patients with accurate medical care. Lack of availability to this data during emergency medical care can lead to life threatening situations therefore placing these items in the high availability category.

[4] What is the financial impact if information were not available when needed?

Example(s): For any SE where online services generate revenue, a disruption of service can have a financial impact which could be deemed severe.

A personal computer system crash which can be solved by a simple reboot would have minimal impact.

[5] What is the impact to the SE mission if information were not available when needed?

Example(s): Public transportation's mission is to get customers quickly and efficiently to various locations. If access to train, bus and subway schedules was unavailable, this could lead to an inability of public transportation to fulfill its mission. The impact to its mission would be severe.

[6] What is the impact to the public trust if the information were not available when needed?

Example(s): SE's have spent considerable effort modernizing operations to include online services and encouraging the public to use these services. If these services are seriously degraded or disrupted, this could cause serious embarrassment to the SE resulting in a severe impact. The availability in this case would be high.

2.3 Instructions for Using the Information Classification Worksheet

An Information Classification Worksheet is provided in Appendix C consisting of the confidentiality, integrity, and availability (CIA) questions previously presented. The objective of the worksheet is to identify information assets and to determine whether the information asset rates low, moderate, or high for CIA. The information owner answers the

questions for each category until the information is classified for that category. Once the worksheet is complete, an overall classification rating is achieved for the information asset (e.g., confidentiality – high, integrity – moderate, availability – low). If needed, the information owner can refer back to this Manual for clarification and examples for each of the questions on the worksheet.

3. Determination of Controls

Once the information is classified, baseline controls are determined using the control charts. Control charts have been created corresponding to the CIA levels. For instance, if after answering the questions on page 2 of the **Information Asset Classification Worksheet**, the information asset is classified as confidentiality – high, integrity – moderate, availability – low then you would refer to the associated confidentiality – high, integrity – moderate, availability – low (i.e., HML) control chart.

There are five primary roles depicted on the control charts:

- State Entity (SE);
- Information Owner;
- Information Custodian;
- SE Workforce (Information User); and
- Information Security Officer (ISO).

The control charts were designed to separate controls based on role. For example, information owners can determine the responsibilities they have by referring to the “Information Owner Controls” section of the appropriate control chart for the information asset being classified.

The control charts *suggest* the roles where a control should be assigned. Based on the structure of the SE’s organization, the responsibility for the control may be better suited to another role as determined by the SE. Note, that individuals may have multiple roles.

In total, there are 27 different control charts in Appendix D. The control charts contain the baseline controls that must be implemented based on the information classification. A SE may add more controls but may not alter or remove the original controls. In addition to the 27 control charts, Appendix D includes one page summaries for all confidentiality controls, all integrity controls and all availability controls. As a reminder, all SE’s are required to comply with Information Security Policy P03-002.

An alphabetical **Glossary of Information Security Controls** is provided in Appendix E to offer clarification on each control. The Glossary should be used in conjunction with the control charts.

An electronic version of Appendices D and E is available at www.dhSES.ny.gov/ocs/resources/. The control charts and glossary provided are formatted in Excel and have the following features:

- all 27 classification ratings are hyperlinked to the appropriate control chart;
- each control in the control charts is hyperlinked to the appropriate entry in the **Glossary of Information Security Controls**; and
- the ALT + LEFT ARROW keys can be used to return to a previous page for ease of navigation in the spreadsheet.

Closing

Information classification is a necessary part of information security management in an organization. The purpose of this Manual has been to facilitate policy implementation by offering a step-by-step process which can be followed by an information owner. The process has been divided into three steps:

1. information asset identification;
2. information asset classification; and
3. control selection.

For information asset identification, a template has been provided to collect relevant pieces of information to assist in classification. Information asset classification has been simplified by the use of the provided structured questionnaire. Information owners answer a series of questions until they conclusively determine the classification level. The Manual also provides clarification and examples for each of the classification questions. The process of selecting controls for the classified information has also been detailed.

The classification process that has been described in this Manual is meant to be used to determine the controls, but not the specific procedures for control implementation. It should also be noted that the Manual is to be used as a tool to assist SEs in complying with the Information Classification and Control Standard and is not the actual standard itself.

Information Classification and Control Appendix C

Information Asset Classification Worksheet

Original Publication Date: October 10, 2008
Revision Date: February 7, 2012

INFORMATION ASSET CLASSIFICATION WORKSHEET

INFORMATION ASSET IDENTIFICATION

Completed By:	
Completed Date:	
Department:	
Name of Information Asset:	
Information Asset Description/Comment:	
Information Asset Use: <small>(What business need does the information asset satisfy?)</small>	
Information Asset Format: <small>(i.e., paper, electronic)</small>	
Information Asset Storage: <small>(e.g., file cabinet, safe, database, network share, CD/DVD, portable drive)</small>	
Source of Information:	
Business Process(es) Supported:	
Information Owner:	
Information Custodian:	
Internal Information User(s):	
External Information User(s): <small>(e.g., other State Agencies, other governmental agencies, public)</small>	
Information Asset ID Number:	

Instructions:

On page one, record the requested information for the information asset you are classifying. Job titles, in place of named individuals, can be used where appropriate for ease of maintenance. On page two, answer the questions in each column (Confidentiality, Integrity and Availability) sequentially. If your answer gives you a classification for that category (e.g., confidentiality is high), record the classification at the bottom of the worksheet and follow the directions to either move to the next column or complete the classification rating. If you answer all questions in one column without being given a classification, follow the instructions at the bottom of the worksheet and record the classification before moving on to the next column or completing the worksheet. Once you have a classification rating for all three categories (Confidentiality - C, Integrity - I, Availability - A), refer to the appropriate control chart. Please note, you may answer all questions in a column. This practice may provide you with a better understanding of the risks associated with the information asset.

For further information on minimal, limited and severe impact refer to the Information Classification and Control Policy and Standard.

CONFIDENTIALITY QUESTIONS	INTEGRITY QUESTIONS	AVAILABILITY QUESTIONS
<p>1 Does the information include or contain PPSI (Personal, Private, or Sensitive Information)?</p> <p>A) No - continue with Confidentiality questions D) Yes - Confidentiality is High (rate below), continue with Integrity questions</p> <p>2 What impact does unauthorized access or disclosure of information have on health and safety?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions</p> <p>3 What is the financial impact of unauthorized access or disclosure of information?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions</p> <p>4 What impact does unauthorized access or disclosure of information have on the SE mission?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions</p> <p>5 What impact does unauthorized access or disclosure of information have on the public trust?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions</p> <p>6 Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or disclosure of information.</p> <p>A) No - continue with Confidentiality questions B) Yes - Minimal impact - continue with Confidentiality questions C) Yes - Limited impact - continue with Confidentiality questions D) Yes - Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p> <p>7 Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure.</p> <p>A) No - continue with Confidentiality questions B) Yes - Minimal impact - continue with Confidentiality questions C) Yes - Limited impact - continue with Confidentiality questions D) Yes - Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p> <p>8 Is the information publicly available?</p> <p>A) No - see Instructions below, then continue with Integrity questions B) Yes - see Instructions below, then continue with Integrity questions</p>	<p>1 Does the information include medical records?</p> <p>A) No - continue with Integrity questions D) Yes - Integrity is High (rate below), continue with Availability questions</p> <p>2 Is the information (e.g., security logs) relied upon to make critical security decisions ?</p> <p>A) No - continue with Integrity questions D) Yes - Integrity is High (rate below), continue with Availability questions</p> <p>3 What impact does unauthorized modification or destruction of information have on health and safety?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe Impact - Integrity is High (rate below), continue with Availability questions</p> <p>4 What is the financial impact of unauthorized modification or destruction of information?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe Impact - Integrity is High (rate below), continue with Availability questions</p> <p>5 What impact does unauthorized modification or destruction of information have on the SE mission?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe Impact - Integrity is High (rate below), continue with Availability questions</p> <p>6 What impact does unauthorized modification or destruction of information have on the public trust?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p> <p>7 Is integrity addressed by law or regulation? If yes, determine the impact of unauthorized modification or destruction of information.</p> <p>A) No - continue with Integrity questions B) Yes - Minimal impact - continue with Integrity questions C) Yes - Limited impact - continue with Integrity questions D) Yes - Severe impact - Integrity is High (rate below), continue with Availability ques.</p> <p>8 Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, determine the impact of unauthorized modification or destruction of information.</p> <p>A) No - see Instructions below then continue with Availability questions B) Yes - Minimal impact - see Instructions below then continue with Availability ques. C) Yes - Limited impact - see Instructions below then continue with Availability ques. D) Yes - Severe impact - Integrity is High (rate below), continue with Availability ques.</p>	<p>1 Is availability of the information essential for emergency response or disaster recovery?</p> <p>A) No - continue with Availability questions D) Yes - Availability is High (rate below)</p> <p>2 This information needs to be provided or available:</p> <p>A) As time permits - continue with Availability questions C) Within 1 to 7 days - continue with Availability questions D) 24 hrs. per day/7 days a week - Availability is High (rate below)</p> <p>3 What is the impact to health and safety if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe Impact - Availability is High (rate below)</p> <p>4 What is the financial impact if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe Impact - Availability is High (rate below)</p> <p>5 What is the impact to the SE mission if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe Impact - Availability is High (rate below)</p> <p>6 What is the impact to the public trust if the information were not available when needed?</p> <p>A) None - see Instructions below B) Minimal impact - see Instructions below C) Limited impact - see Instructions below D) Severe impact - Availability is High (rate below)</p>

INSTRUCTIONS FOR RATING EACH COLUMN:

If ALL of the above answers are **A/B (GREEN)**, rating is **LOW**; if ANY of the above answers are **C (YELLOW)** and NONE are **D (RED)**, rating is **MODERATE**; if ANY of the above answers are **D (RED)**, rating is **HIGH**

SCALE: **A/B = GREEN = LOW** **C = YELLOW = MODERATE** **D = RED = HIGH**

CLASSIFICATION RATING FOR CONFIDENTIALITY:

CLASSIFICATION RATING FOR INTEGRITY:

CLASSIFICATION RATING FOR AVAILABILITY:

Information Classification and Control Appendix D

Information Control Charts

Original Publication Date: October 10, 2008
Revision Date: February 7, 2012

**Information Control Charts
Classification Rating Menu**

Page #	Classification Rating	Confidentiality	Integrity	Availability
1-	LLL	Low	Low	Low
2-	LLM	Low	Low	Moderate
3-	LLH	Low	Low	High
4-	LML	Low	Moderate	Low
5-	LMM	Low	Moderate	Moderate
6-	LMH	Low	Moderate	High
7-	LHL	Low	High	Low
8-	LHM	Low	High	Moderate
9-	LHH	Low	High	High
10-	MLL	Moderate	Low	Low
11-	MLM	Moderate	Low	Moderate
12-	MLH	Moderate	Low	High
13-	MML	Moderate	Moderate	Low
14-	MMM	Moderate	Moderate	Moderate
15-	MMH	Moderate	Moderate	High
16-	MHL	Moderate	High	Low
17-	MHM	Moderate	High	Moderate
18-	MHH	Moderate	High	High
19-	HLL	High	Low	Low
20-	HLM	High	Low	Moderate
21-	HLH	High	Low	High
22-	HML	High	Moderate	Low
23-	HMM	High	Moderate	Moderate
24-	HMH	High	Moderate	High
25-	HHL	High	High	Low
26-	HHM	High	High	Moderate
27-	HHH	High	High	High
28-	Confidentiality Controls			
29-	Integrity Controls			
30-	Availability Controls			

CONFIDENTIALITY (C): LOW		INTEGRITY (I): LOW		AVAILABILITY (A): LOW	
Glossary X-Ref #	R=Required O=Optional				CIA
STATE ENTITY (SE) CONTROLS					
2	R Access approval/removal process in place				C
29	R Information classification and inventory				CIA
38	R Privacy disclaimer on e-mail and fax cover sheets				C
INFORMATION OWNER CONTROLS					
3	R Access authorized by information owner				C
43	R Review access lists				CI
45	R Review and reclassify information				CIA
INFORMATION CUSTODIAN CONTROLS					
12	R Basic input data validation				I
22	R Erase re-writeable media prior to reuse				C
25	O IAM Trust Level 1 for information systems				CI
55	R Use disposal method for re-writeable media				C
SE WORKFORCE (INFORMATION USER) CONTROLS					
31	O Label: "NYS CONFIDENTIALITY-LOW"				C
54	R Use disposal method for paper or write-once media				C
INFORMATION SECURITY OFFICER (ISO) CONTROLS					
46	R Review security procedures and controls				CIA

CONFIDENTIALITY (C): LOW		INTEGRITY (I): LOW		AVAILABILITY (A): MODERATE	
Glossary X-Ref #	R=Required O=Optional				CIA
STATE ENTITY (SE) CONTROLS					
2	R Access approval/removal process in place				C
29	R Information classification and inventory				CIA
38	R Privacy disclaimer on e-mail and fax cover sheets				C
INFORMATION OWNER CONTROLS					
3	R Access authorized by information owner				C
6	R Access provided to more than one person				A
43	R Review access lists				CI
45	R Review and reclassify information				CIA
INFORMATION CUSTODIAN CONTROLS					
11	R Backup recovery procedures				IA
12	R Basic input data validation				I
20	R Environmental protection measures				IA
22	R Erase re-writeable media prior to reuse				C
25	O IAM Trust Level 1 for information systems				CI
39	R Regular backup				IA
55	R Use disposal method for re-writeable media				C
SE WORKFORCE (INFORMATION USER) CONTROLS					
31	O Label: "NYS CONFIDENTIALITY-LOW"				C
54	R Use disposal method for paper or write-once media				C
INFORMATION SECURITY OFFICER (ISO) CONTROLS					
46	R Review security procedures and controls				CIA

CONFIDENTIALITY (C): LOW		INTEGRITY (I): LOW		AVAILABILITY (A): HIGH	
Glossary X-Ref #	R=Required O=Optional				CIA
STATE ENTITY (SE) CONTROLS					
2	R Access approval/removal process in place				C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan				A
29	R Information classification and inventory				CIA
38	R Privacy disclaimer on e-mail and fax cover sheets				C
INFORMATION OWNER CONTROLS					
3	R Access authorized by information owner				C
6	R Access provided to more than one person				A
43	R Review access lists				CI
45	R Review and reclassify information				CIA
INFORMATION CUSTODIAN CONTROLS					
8	R Alternate means of availability				A
11	R Backup recovery procedures				IA
12	R Basic input data validation				I
20	R Environmental protection measures				IA
21	R Environmental protection measures monitoring				IA
22	R Erase re-writeable media prior to reuse				C
25	O IAM Trust Level 1 for information systems				CI
37	R Off-site backup				A
39	R Regular backup				IA
52	R Test recovery of backup data				IA
55	R Use disposal method for re-writeable media				C
SE WORKFORCE (INFORMATION USER) CONTROLS					
31	O Label: "NYS CONFIDENTIALITY-LOW"				C
54	R Use disposal method for paper or write-once media				C
INFORMATION SECURITY OFFICER (ISO) CONTROLS					
47	R Review security procedures and controls (annually)				CIA

CONFIDENTIALITY (C): LOW		INTEGRITY (I): MODERATE	AVAILABILITY (A): LOW	
Glossary X-Ref #	R=Required O=Optional			CIA
STATE ENTITY (SE) CONTROLS				
2	R Access approval/removal process in place			C
23	R Formal change control procedures for information systems			I
24	R Formal test plans and documented results for information systems			I
29	R Information classification and inventory			CIA
38	R Privacy disclaimer on e-mail and fax cover sheets			C
INFORMATION OWNER CONTROLS				
3	R Access authorized by information owner			C
43	R Review access lists			CI
45	R Review and reclassify information			CIA
INFORMATION CUSTODIAN CONTROLS				
11	R Backup recovery procedures			IA
12	R Basic input data validation			I
16	R Data plausibility and field comparison edits			I
20	R Environmental protection measures			IA
22	R Erase re-writeable media prior to reuse			C
26	R IAM Trust Level 2 for information systems			CI
39	R Regular backup			IA
55	R Use disposal method for re-writeable media			C
SE WORKFORCE (INFORMATION USER) CONTROLS				
31	O Label: "NYS CONFIDENTIALITY-LOW"			C
49	R Secure area			CI
54	R Use disposal method for paper or write-once media			C
INFORMATION SECURITY OFFICER (ISO) CONTROLS				
46	R Review security procedures and controls			CIA

CONFIDENTIALITY (C): LOW		INTEGRITY (I): MODERATE	AVAILABILITY (A): MODERATE
Glossary	R=Required O=Optional		CIA
X-Ref #			
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
23	R Formal change control procedures for information systems		I
24	R Formal test plans and documented results for information systems		I
29	R Information classification and inventory		CIA
38	R Privacy disclaimer on e-mail and fax cover sheets		C
INFORMATION OWNER CONTROLS			
3	R Access authorized by information owner		C
6	R Access provided to more than one person		A
43	R Review access lists		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
11	R Backup recovery procedures		IA
12	R Basic input data validation		I
16	R Data plausibility and field comparison edits		I
20	R Environmental protection measures		IA
22	R Erase re-writeable media prior to reuse		C
26	R IAM Trust Level 2 for information systems		CI
39	R Regular backup		IA
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
31	O Label: "NYS CONFIDENTIALITY-LOW"		C
49	R Secure area		CI
54	R Use disposal method for paper or write-once media		C
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
46	R Review security procedures and controls		CIA

CONFIDENTIALITY (C): LOW		INTEGRITY (I): MODERATE	AVAILABILITY (A): HIGH
Glossary X-Ref #	R=Required O=Optional	CIA	
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place	C	
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan	A	
23	R Formal change control procedures for information systems	I	
24	R Formal test plans and documented results for information systems	I	
29	R Information classification and inventory	CIA	
38	R Privacy disclaimer on e-mail and fax cover sheets	C	
INFORMATION OWNER CONTROLS			
3	R Access authorized by information owner	C	
6	R Access provided to more than one person	A	
43	R Review access lists	CI	
45	R Review and reclassify information	CIA	
INFORMATION CUSTODIAN CONTROLS			
8	R Alternate means of availability	A	
11	R Backup recovery procedures	IA	
12	R Basic input data validation	I	
16	R Data plausibility and field comparison edits	I	
20	R Environmental protection measures	IA	
21	R Environmental protection measures monitoring	IA	
22	R Erase re-writeable media prior to reuse	C	
26	R IAM Trust Level 2 for information systems	CI	
37	R Off-site backup	A	
39	R Regular backup	IA	
52	R Test recovery of backup data	IA	
55	R Use disposal method for re-writeable media	C	
SE WORKFORCE (INFORMATION USER) CONTROLS			
31	O Label: "NYS CONFIDENTIALITY-LOW"	C	
49	R Secure area	CI	
54	R Use disposal method for paper or write-once media	C	
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
47	R Review security procedures and controls (annually)	CIA	

CONFIDENTIALITY (C): LOW		INTEGRITY (I): HIGH	AVAILABILITY (A): LOW	
Glossary X-Ref #	R=Required O=Optional			CIA
STATE ENTITY (SE) CONTROLS				
2	R Access approval/removal process in place			C
10	R Approved storage facility			CI
23	R Formal change control procedures for information systems			I
24	R Formal test plans and documented results for information systems			I
29	R Information classification and inventory			CIA
38	R Privacy disclaimer on e-mail and fax cover sheets			C
48	R Review system and application security logs			CI
INFORMATION OWNER CONTROLS				
3	R Access authorized by information owner			C
44	R Review access lists (annually)			CI
45	R Review and reclassify information			CIA
INFORMATION CUSTODIAN CONTROLS				
11	R Backup recovery procedures			IA
12	R Basic input data validation			I
16	R Data plausibility and field comparison edits			I
20	R Environmental protection measures			IA
21	R Environmental protection measures monitoring			IA
22	R Erase re-writeable media prior to reuse			C
27	R IAM Trust Level 3 for information systems			CI
28	O IAM Trust Level 4 for information systems			CI
33	R Limit access to secure areas			CI
34	R Message integrity			I
39	R Regular backup			IA
52	R Test recovery of backup data			IA
55	R Use disposal method for re-writeable media			C
SE WORKFORCE (INFORMATION USER) CONTROLS				
31	O Label: "NYS CONFIDENTIALITY-LOW"			C
49	R Secure area			CI
50	R Secure physical media when unattended			CI
54	R Use disposal method for paper or write-once media			C
INFORMATION SECURITY OFFICER (ISO) CONTROLS				
47	R Review security procedures and controls (annually)			CIA

CONFIDENTIALITY (C): LOW		INTEGRITY (I): HIGH		AVAILABILITY (A): MODERATE	
Glossary X-Ref #	R=Required O=Optional				CIA
STATE ENTITY (SE) CONTROLS					
2	R Access approval/removal process in place				C
10	R Approved storage facility				CI
23	R Formal change control procedures for information systems				I
24	R Formal test plans and documented results for information systems				I
29	R Information classification and inventory				CIA
38	R Privacy disclaimer on e-mail and fax cover sheets				C
48	R Review system and application security logs				CI
INFORMATION OWNER CONTROLS					
3	R Access authorized by information owner				C
6	R Access provided to more than one person				A
44	R Review access lists (annually)				CI
45	R Review and reclassify information				CIA
INFORMATION CUSTODIAN CONTROLS					
11	R Backup recovery procedures				IA
12	R Basic input data validation				I
16	R Data plausibility and field comparison edits				I
20	R Environmental protection measures				IA
21	R Environmental protection measures monitoring				IA
22	R Erase re-writeable media prior to reuse				C
27	R IAM Trust Level 3 for information systems				CI
28	O IAM Trust Level 4 for information systems				CI
33	R Limit access to secure areas				CI
34	R Message integrity				I
39	R Regular backup				IA
52	R Test recovery of backup data				IA
55	R Use disposal method for re-writeable media				C
SE WORKFORCE (INFORMATION USER) CONTROLS					
31	O Label: "NYS CONFIDENTIALITY-LOW"				C
49	R Secure area				CI
50	R Secure physical media when unattended				CI
54	R Use disposal method for paper or write-once media				C
INFORMATION SECURITY OFFICER (ISO) CONTROLS					
47	R Review security procedures and controls (annually)				CIA

CONFIDENTIALITY (C): LOW		INTEGRITY (I): HIGH	AVAILABILITY (A): HIGH
Glossary X-Ref #	R=Required O=Optional	CIA	
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan		A
10	R Approved storage facility		CI
23	R Formal change control procedures for information systems		I
24	R Formal test plans and documented results for information systems		I
29	R Information classification and inventory		CIA
38	R Privacy disclaimer on e-mail and fax cover sheets		C
48	R Review system and application security logs		CI
INFORMATION OWNER CONTROLS			
3	R Access authorized by information owner		C
6	R Access provided to more than one person		A
44	R Review access lists (annually)		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
8	R Alternate means of availability		A
11	R Backup recovery procedures		IA
12	R Basic input data validation		I
16	R Data plausibility and field comparison edits		I
20	R Environmental protection measures		IA
21	R Environmental protection measures monitoring		IA
22	R Erase re-writeable media prior to reuse		C
27	R IAM Trust Level 3 for information systems		CI
28	O IAM Trust Level 4 for information systems		CI
33	R Limit access to secure areas		CI
34	R Message integrity		I
37	R Off-site backup		A
39	R Regular backup		IA
52	R Test recovery of backup data		IA
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
31	O Label: "NYS CONFIDENTIALITY-LOW"		C
49	R Secure area		CI
50	R Secure physical media when unattended		CI
54	R Use disposal method for paper or write-once media		C
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
47	R Review security procedures and controls (annually)		CIA

CONFIDENTIALITY (C): MODERATE		INTEGRITY (I): LOW	AVAILABILITY (A): LOW
Glossary	R=Required O=Optional		CIA
X-Ref #			
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
17	R Destroy when no longer needed		C
29	R Information classification and inventory		CIA
38	R Privacy disclaimer on e-mail and fax cover sheets		C
INFORMATION OWNER CONTROLS			
4	R Access authorized by information owner (written)		C
43	R Review access lists		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
12	R Basic input data validation		I
22	R Erase re-writeable media prior to reuse		C
26	R IAM Trust Level 2 for information systems		CI
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
14	R Conceal physical media		C
15	R Confirmation of identity and access rights of requester		C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"		C
42	R Retrieval when printing/faxing (timely)		C
49	R Secure area		CI
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
46	R Review security procedures and controls		CIA

CONFIDENTIALITY (C): MODERATE		INTEGRITY (I): LOW	AVAILABILITY (A): MODERATE	
Glossary X-Ref #	R=Required O=Optional			CIA
STATE ENTITY (SE) CONTROLS				
2	R Access approval/removal process in place			C
17	R Destroy when no longer needed			C
29	R Information classification and inventory			CIA
38	R Privacy disclaimer on e-mail and fax cover sheets			C
INFORMATION OWNER CONTROLS				
4	R Access authorized by information owner (written)			C
6	R Access provided to more than one person			A
43	R Review access lists			CI
45	R Review and reclassify information			CIA
INFORMATION CUSTODIAN CONTROLS				
11	R Backup recovery procedures			IA
12	R Basic input data validation			I
20	R Environmental protection measures			IA
22	R Erase re-writeable media prior to reuse			C
26	R IAM Trust Level 2 for information systems			CI
39	R Regular backup			IA
55	R Use disposal method for re-writeable media			C
SE WORKFORCE (INFORMATION USER) CONTROLS				
14	R Conceal physical media			C
15	R Confirmation of identity and access rights of requester			C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"			C
42	R Retrieval when printing/faxing (timely)			C
49	R Secure area			CI
INFORMATION SECURITY OFFICER (ISO) CONTROLS				
46	R Review security procedures and controls			CIA

CONFIDENTIALITY (C): MODERATE		INTEGRITY (I): LOW	AVAILABILITY (A): HIGH
Glossary	R=Required O=Optional		CIA
X-Ref #			
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan		A
17	R Destroy when no longer needed		C
29	R Information classification and inventory		CIA
38	R Privacy disclaimer on e-mail and fax cover sheets		C
INFORMATION OWNER CONTROLS			
4	R Access authorized by information owner (written)		C
6	R Access provided to more than one person		A
43	R Review access lists		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
8	R Alternate means of availability		A
11	R Backup recovery procedures		IA
12	R Basic input data validation		I
20	R Environmental protection measures		IA
21	R Environmental protection measures monitoring		IA
22	R Erase re-writeable media prior to reuse		C
26	R IAM Trust Level 2 for information systems		CI
37	R Off-site backup		A
39	R Regular backup		IA
52	R Test recovery of backup data		IA
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
14	R Conceal physical media		C
15	R Confirmation of identity and access rights of requester		C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"		C
42	R Retrieval when printing/faxing (timely)		C
49	R Secure area		CI
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
47	R Review security procedures and controls (annually)		CIA

CONFIDENTIALITY (C): MODERATE		INTEGRITY (I): MODERATE	AVAILABILITY (A): LOW
Glossary	R=Required O=Optional		CIA
X-Ref #			
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
17	R Destroy when no longer needed		C
23	R Formal change control procedures for information systems		I
24	R Formal test plans and documented results for information systems		I
29	R Information classification and inventory		CIA
38	R Privacy disclaimer on e-mail and fax cover sheets		C
INFORMATION OWNER CONTROLS			
4	R Access authorized by information owner (written)		C
43	R Review access lists		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
11	R Backup recovery procedures		IA
12	R Basic input data validation		I
16	R Data plausibility and field comparison edits		I
20	R Environmental protection measures		IA
22	R Erase re-writeable media prior to reuse		C
26	R IAM Trust Level 2 for information systems		CI
39	R Regular backup		IA
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
14	R Conceal physical media		C
15	R Confirmation of identity and access rights of requester		C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"		C
42	R Retrieval when printing/faxing (timely)		C
49	R Secure area		CI
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
46	R Review security procedures and controls		CIA

CONFIDENTIALITY (C): MODERATE		INTEGRITY (I): MODERATE	AVAILABILITY (A): MODERATE
Glossary X-Ref #	R=Required O=Optional		CIA
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
17	R Destroy when no longer needed		C
23	R Formal change control procedures for information systems		I
24	R Formal test plans and documented results for information systems		I
29	R Information classification and inventory		CIA
38	R Privacy disclaimer on e-mail and fax cover sheets		C
INFORMATION OWNER CONTROLS			
4	R Access authorized by information owner (written)		C
6	R Access provided to more than one person		A
43	R Review access lists		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
11	R Backup recovery procedures		IA
12	R Basic input data validation		I
16	R Data plausibility and field comparison edits		I
20	R Environmental protection measures		IA
22	R Erase re-writeable media prior to reuse		C
26	R IAM Trust Level 2 for information systems		CI
39	R Regular backup		IA
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
14	R Conceal physical media		C
15	R Confirmation of identity and access rights of requester		C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"		C
42	R Retrieval when printing/faxing (timely)		C
49	R Secure area		CI
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
46	R Review security procedures and controls		CIA

CONFIDENTIALITY (C): MODERATE		INTEGRITY (I): MODERATE	AVAILABILITY (A): HIGH
Glossary X-Ref #	R=Required O=Optional		CIA
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan		A
17	R Destroy when no longer needed		C
23	R Formal change control procedures for information systems		I
24	R Formal test plans and documented results for information systems		I
29	R Information classification and inventory		CIA
38	R Privacy disclaimer on e-mail and fax cover sheets		C
INFORMATION OWNER CONTROLS			
4	R Access authorized by information owner (written)		C
6	R Access provided to more than one person		A
43	R Review access lists		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
8	R Alternate means of availability		A
11	R Backup recovery procedures		IA
12	R Basic input data validation		I
16	R Data plausibility and field comparison edits		I
20	R Environmental protection measures		IA
21	R Environmental protection measures monitoring		IA
22	R Erase re-writeable media prior to reuse		C
26	R IAM Trust Level 2 for information systems		CI
37	R Off-site backup		A
39	R Regular backup		IA
52	R Test recovery of backup data		IA
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
14	R Conceal physical media		C
15	R Confirmation of identity and access rights of requester		C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"		C
42	R Retrieval when printing/faxing (timely)		C
49	R Secure area		CI
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
47	R Review security procedures and controls (annually)		CIA

CONFIDENTIALITY (C): MODERATE		INTEGRITY (I): HIGH	AVAILABILITY (A): LOW
Glossary X-Ref #	R=Required O=Optional	CIA	
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place	C	
10	R Approved storage facility	CI	
17	R Destroy when no longer needed	C	
23	R Formal change control procedures for information systems	I	
24	R Formal test plans and documented results for information systems	I	
29	R Information classification and inventory	CIA	
38	R Privacy disclaimer on e-mail and fax cover sheets	C	
48	R Review system and application security logs	CI	
INFORMATION OWNER CONTROLS			
4	R Access authorized by information owner (written)	C	
44	R Review access lists (annually)	CI	
45	R Review and reclassify information	CIA	
INFORMATION CUSTODIAN CONTROLS			
11	R Backup recovery procedures	IA	
12	R Basic input data validation	I	
16	R Data plausibility and field comparison edits	I	
20	R Environmental protection measures	IA	
21	R Environmental protection measures monitoring	IA	
22	R Erase re-writeable media prior to reuse	C	
27	R IAM Trust Level 3 for information systems	CI	
28	O IAM Trust Level 4 for information systems	CI	
33	R Limit access to secure areas	CI	
34	R Message integrity	I	
39	R Regular backup	IA	
52	R Test recovery of backup data	IA	
55	R Use disposal method for re-writeable media	C	
SE WORKFORCE (INFORMATION USER) CONTROLS			
15	R Confirmation of identity and access rights of requester	C	
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	C	
42	R Retrieval when printing/faxing (timely)	C	
49	R Secure area	CI	
50	R Secure physical media when unattended	CI	
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
47	R Review security procedures and controls (annually)	CIA	

CONFIDENTIALITY (C): MODERATE		INTEGRITY (I): HIGH	AVAILABILITY (A): MODERATE	
Glossary X-Ref #	R=Required O=Optional			CIA
STATE ENTITY (SE) CONTROLS				
2	R Access approval/removal process in place			C
10	R Approved storage facility			CI
17	R Destroy when no longer needed			C
23	R Formal change control procedures for information systems			I
24	R Formal test plans and documented results for information systems			I
29	R Information classification and inventory			CIA
38	R Privacy disclaimer on e-mail and fax cover sheets			C
48	R Review system and application security logs			CI
INFORMATION OWNER CONTROLS				
4	R Access authorized by information owner (written)			C
6	R Access provided to more than one person			A
44	R Review access lists (annually)			CI
45	R Review and reclassify information			CIA
INFORMATION CUSTODIAN CONTROLS				
11	R Backup recovery procedures			IA
12	R Basic input data validation			I
16	R Data plausibility and field comparison edits			I
20	R Environmental protection measures			IA
21	R Environmental protection measures monitoring			IA
22	R Erase re-writeable media prior to reuse			C
27	R IAM Trust Level 3 for information systems			CI
28	O IAM Trust Level 4 for information systems			CI
33	R Limit access to secure areas			CI
34	R Message integrity			I
39	R Regular backup			IA
52	R Test recovery of backup data			IA
55	R Use disposal method for re-writeable media			C
SE WORKFORCE (INFORMATION USER) CONTROLS				
15	R Confirmation of identity and access rights of requester			C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"			C
42	R Retrieval when printing/faxing (timely)			C
49	R Secure area			CI
50	R Secure physical media when unattended			CI
INFORMATION SECURITY OFFICER (ISO) CONTROLS				
47	R Review security procedures and controls (annually)			CIA

CONFIDENTIALITY (C): MODERATE		INTEGRITY (I): HIGH	AVAILABILITY (A): HIGH
Glossary X-Ref #	R=Required O=Optional	CIA	
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan		A
10	R Approved storage facility		CI
17	R Destroy when no longer needed		C
23	R Formal change control procedures for information systems		I
24	R Formal test plans and documented results for information systems		I
29	R Information classification and inventory		CIA
38	R Privacy disclaimer on e-mail and fax cover sheets		C
48	R Review system and application security logs		CI
INFORMATION OWNER CONTROLS			
4	R Access authorized by information owner (written)		C
6	R Access provided to more than one person		A
44	R Review access lists (annually)		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
8	R Alternate means of availability		A
11	R Backup recovery procedures		IA
12	R Basic input data validation		I
16	R Data plausibility and field comparison edits		I
20	R Environmental protection measures		IA
21	R Environmental protection measures monitoring		IA
22	R Erase re-writeable media prior to reuse		C
27	R IAM Trust Level 3 for information systems		CI
28	O IAM Trust Level 4 for information systems		CI
33	R Limit access to secure areas		CI
34	R Message integrity		I
37	R Off-site backup		A
39	R Regular backup		IA
52	R Test recovery of backup data		IA
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
15	R Confirmation of identity and access rights of requester		C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"		C
42	R Retrieval when printing/faxing (timely)		C
49	R Secure area		CI
50	R Secure physical media when unattended		CI
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
47	R Review security procedures and controls (annually)		CIA

CONFIDENTIALITY (C): HIGH		INTEGRITY (I): LOW	AVAILABILITY (A): LOW
Glossary X-Ref #	R=Required O=Optional	CIA	
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place	C	
9	R Approved electronic storage media and devices	C	
10	R Approved storage facility	CI	
13	R Chain of custody for physical media	C	
17	R Destroy when no longer needed	C	
29	R Information classification and inventory	CIA	
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C	
38	R Privacy disclaimer on e-mail and fax cover sheets	C	
40	R Reproduction authorized by information owner	C	
48	R Review system and application security logs	CI	
56	R Written approval for Transmission, Transportation and Storage (TTS)	C	
INFORMATION OWNER CONTROLS			
5	R Access authorized by information owner (written & cc: exec)	C	
44	R Review access lists (annually)	CI	
45	R Review and reclassify information	CIA	
INFORMATION CUSTODIAN CONTROLS			
12	R Basic input data validation	I	
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C	
19	R Encryption/hashing of electronic authentication information	C	
22	R Erase re-writeable media prior to reuse	C	
27	R IAM Trust Level 3 for information systems	CI	
28	O IAM Trust Level 4 for information systems	CI	
33	R Limit access to secure areas	CI	
55	R Use disposal method for re-writeable media	C	
SE WORKFORCE (INFORMATION USER) CONTROLS			
15	R Confirmation of identity and access rights of requester	C	
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C	
35	R No confidential information in e-mail subject line	C	
41	R Retrieval when printing/faxing (immediate)	C	
49	R Secure area	CI	
50	R Secure physical media when unattended	CI	
51	R Situational awareness during verbal communications	C	
53	R Transportation handling controls for paper	C	
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
1	R Access approval/removal process (audit)	C	
47	R Review security procedures and controls (annually)	CIA	

CONFIDENTIALITY (C): HIGH		INTEGRITY (I): LOW	AVAILABILITY (A): MODERATE
Glossary X-Ref #	R=Required O=Optional	CIA	
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place	C	
9	R Approved electronic storage media and devices	C	
10	R Approved storage facility	CI	
13	R Chain of custody for physical media	C	
17	R Destroy when no longer needed	C	
29	R Information classification and inventory	CIA	
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C	
38	R Privacy disclaimer on e-mail and fax cover sheets	C	
40	R Reproduction authorized by information owner	C	
48	R Review system and application security logs	CI	
56	R Written approval for Transmission, Transportation and Storage (TTS)	C	
INFORMATION OWNER CONTROLS			
5	R Access authorized by information owner (written & cc: exec)	C	
6	R Access provided to more than one person	A	
44	R Review access lists (annually)	CI	
45	R Review and reclassify information	CIA	
INFORMATION CUSTODIAN CONTROLS			
11	R Backup recovery procedures	IA	
12	R Basic input data validation	I	
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C	
19	R Encryption/hashing of electronic authentication information	C	
20	R Environmental protection measures	IA	
22	R Erase re-writeable media prior to reuse	C	
27	R IAM Trust Level 3 for information systems	CI	
28	O IAM Trust Level 4 for information systems	CI	
33	R Limit access to secure areas	CI	
39	R Regular backup	IA	
55	R Use disposal method for re-writeable media	C	
SE WORKFORCE (INFORMATION USER) CONTROLS			
15	R Confirmation of identity and access rights of requester	C	
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C	
35	R No confidential information in e-mail subject line	C	
41	R Retrieval when printing/faxing (immediate)	C	
49	R Secure area	CI	
50	R Secure physical media when unattended	CI	
51	R Situational awareness during verbal communications	C	
53	R Transportation handling controls for paper	C	
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
1	R Access approval/removal process (audit)	C	
47	R Review security procedures and controls (annually)	CIA	

CONFIDENTIALITY (C): HIGH		INTEGRITY (I): LOW	AVAILABILITY (A): HIGH	
Glossary X-Ref #	R=Required O=Optional			CIA
STATE ENTITY (SE) CONTROLS				
2	R Access approval/removal process in place			C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan			A
9	R Approved electronic storage media and devices			C
10	R Approved storage facility			CI
13	R Chain of custody for physical media			C
17	R Destroy when no longer needed			C
29	R Information classification and inventory			CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties			C
38	R Privacy disclaimer on e-mail and fax cover sheets			C
40	R Reproduction authorized by information owner			C
48	R Review system and application security logs			CI
56	R Written approval for Transmission, Transportation and Storage (TTS)			C
INFORMATION OWNER CONTROLS				
5	R Access authorized by information owner (written & cc: exec)			C
6	R Access provided to more than one person			A
44	R Review access lists (annually)			CI
45	R Review and reclassify information			CIA
INFORMATION CUSTODIAN CONTROLS				
8	R Alternate means of availability			A
11	R Backup recovery procedures			IA
12	R Basic input data validation			I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE			C
19	R Encryption/hashing of electronic authentication information			C
20	R Environmental protection measures			IA
21	R Environmental protection measures monitoring			IA
22	R Erase re-writeable media prior to reuse			C
27	R IAM Trust Level 3 for information systems			CI
28	O IAM Trust Level 4 for information systems			CI
33	R Limit access to secure areas			CI
37	R Off-site backup			A
39	R Regular backup			IA
52	R Test recovery of backup data			IA
55	R Use disposal method for re-writeable media			C
SE WORKFORCE (INFORMATION USER) CONTROLS				
15	R Confirmation of identity and access rights of requester			C
30	O Label: "NYS CONFIDENTIALITY-HIGH"			C
35	R No confidential information in e-mail subject line			C
41	R Retrieval when printing/faxing (immediate)			C
49	R Secure area			CI
50	R Secure physical media when unattended			CI
51	R Situational awareness during verbal communications			C
53	R Transportation handling controls for paper			C
INFORMATION SECURITY OFFICER (ISO) CONTROLS				
1	R Access approval/removal process (audit)			C
47	R Review security procedures and controls (annually)			CIA

CONFIDENTIALITY (C): HIGH		INTEGRITY (I): MODERATE	AVAILABILITY (A): LOW
Glossary X-Ref #	R=Required O=Optional	CIA	
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
9	R Approved electronic storage media and devices		C
10	R Approved storage facility		CI
13	R Chain of custody for physical media		C
17	R Destroy when no longer needed		C
23	R Formal change control procedures for information systems		I
24	R Formal test plans and documented results for information systems		I
29	R Information classification and inventory		CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties		C
38	R Privacy disclaimer on e-mail and fax cover sheets		C
40	R Reproduction authorized by information owner		C
48	R Review system and application security logs		CI
56	R Written approval for Transmission, Transportation and Storage (TTS)		C
INFORMATION OWNER CONTROLS			
5	R Access authorized by information owner (written & cc: exec)		C
44	R Review access lists (annually)		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
11	R Backup recovery procedures		IA
12	R Basic input data validation		I
16	R Data plausibility and field comparison edits		I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE		C
19	R Encryption/hashing of electronic authentication information		C
20	R Environmental protection measures		IA
22	R Erase re-writeable media prior to reuse		C
27	R IAM Trust Level 3 for information systems		CI
28	O IAM Trust Level 4 for information systems		CI
33	R Limit access to secure areas		CI
39	R Regular backup		IA
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
15	R Confirmation of identity and access rights of requester		C
30	O Label: "NYS CONFIDENTIALITY-HIGH"		C
35	R No confidential information in e-mail subject line		C
41	R Retrieval when printing/faxing (immediate)		C
49	R Secure area		CI
50	R Secure physical media when unattended		CI
51	R Situational awareness during verbal communications		C
53	R Transportation handling controls for paper		C
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
1	R Access approval/removal process (audit)		C
47	R Review security procedures and controls (annually)		CIA

CONFIDENTIALITY (C): HIGH		INTEGRITY (I): MODERATE	AVAILABILITY (A): MODERATE
Glossary X-Ref #	R=Required O=Optional	CIA	
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place	C	
9	R Approved electronic storage media and devices	C	
10	R Approved storage facility	CI	
13	R Chain of custody for physical media	C	
17	R Destroy when no longer needed	C	
23	R Formal change control procedures for information systems	I	
24	R Formal test plans and documented results for information systems	I	
29	R Information classification and inventory	CIA	
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C	
38	R Privacy disclaimer on e-mail and fax cover sheets	C	
40	R Reproduction authorized by information owner	C	
48	R Review system and application security logs	CI	
56	R Written approval for Transmission, Transportation and Storage (TTS)	C	
INFORMATION OWNER CONTROLS			
5	R Access authorized by information owner (written & cc: exec)	C	
6	R Access provided to more than one person	A	
44	R Review access lists (annually)	CI	
45	R Review and reclassify information	CIA	
INFORMATION CUSTODIAN CONTROLS			
11	R Backup recovery procedures	IA	
12	R Basic input data validation	I	
16	R Data plausibility and field comparison edits	I	
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C	
19	R Encryption/hashing of electronic authentication information	C	
20	R Environmental protection measures	IA	
22	R Erase re-writeable media prior to reuse	C	
27	R IAM Trust Level 3 for information systems	CI	
28	O IAM Trust Level 4 for information systems	CI	
33	R Limit access to secure areas	CI	
39	R Regular backup	IA	
55	R Use disposal method for re-writeable media	C	
SE WORKFORCE (INFORMATION USER) CONTROLS			
15	R Confirmation of identity and access rights of requester	C	
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C	
35	R No confidential information in e-mail subject line	C	
41	R Retrieval when printing/faxing (immediate)	C	
49	R Secure area	CI	
50	R Secure physical media when unattended	CI	
51	R Situational awareness during verbal communications	C	
53	R Transportation handling controls for paper	C	
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
1	R Access approval/removal process (audit)	C	
47	R Review security procedures and controls (annually)	CIA	

CONFIDENTIALITY (C): HIGH		INTEGRITY (I): MODERATE	AVAILABILITY (A): HIGH
Glossary X-Ref #	R=Required O=Optional		CIA
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan		A
9	R Approved electronic storage media and devices		C
10	R Approved storage facility		CI
13	R Chain of custody for physical media		C
17	R Destroy when no longer needed		C
23	R Formal change control procedures for information systems		I
24	R Formal test plans and documented results for information systems		I
29	R Information classification and inventory		CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties		C
38	R Privacy disclaimer on e-mail and fax cover sheets		C
40	R Reproduction authorized by information owner		C
48	R Review system and application security logs		CI
56	R Written approval for Transmission, Transportation and Storage (TTS)		C
INFORMATION OWNER CONTROLS			
5	R Access authorized by information owner (written & cc: exec)		C
6	R Access provided to more than one person		A
44	R Review access lists (annually)		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
8	R Alternate means of availability		A
11	R Backup recovery procedures		IA
12	R Basic input data validation		I
16	R Data plausibility and field comparison edits		I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE		C
19	R Encryption/hashing of electronic authentication information		C
20	R Environmental protection measures		IA
21	R Environmental protection measures monitoring		IA
22	R Erase re-writeable media prior to reuse		C
27	R IAM Trust Level 3 for information systems		CI
28	O IAM Trust Level 4 for information systems		CI
33	R Limit access to secure areas		CI
37	R Off-site backup		A
39	R Regular backup		IA
52	R Test recovery of backup data		IA
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
15	R Confirmation of identity and access rights of requester		C
30	O Label: "NYS CONFIDENTIALITY-HIGH"		C
35	R No confidential information in e-mail subject line		C
41	R Retrieval when printing/faxing (immediate)		C
49	R Secure area		CI
50	R Secure physical media when unattended		CI
51	R Situational awareness during verbal communications		C
53	R Transportation handling controls for paper		C
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
1	R Access approval/removal process (audit)		C
47	R Review security procedures and controls (annually)		CIA

CONFIDENTIALITY (C): HIGH		INTEGRITY (I): HIGH		AVAILABILITY (A): LOW	
Glossary X-Ref #	R=Required O=Optional				CIA
STATE ENTITY (SE) CONTROLS					
2	R Access approval/removal process in place				C
9	R Approved electronic storage media and devices				C
10	R Approved storage facility				CI
13	R Chain of custody for physical media				C
17	R Destroy when no longer needed				C
23	R Formal change control procedures for information systems				I
24	R Formal test plans and documented results for information systems				I
29	R Information classification and inventory				CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties				C
38	R Privacy disclaimer on e-mail and fax cover sheets				C
40	R Reproduction authorized by information owner				C
48	R Review system and application security logs				CI
56	R Written approval for Transmission, Transportation and Storage (TTS)				C
INFORMATION OWNER CONTROLS					
5	R Access authorized by information owner (written & cc: exec)				C
44	R Review access lists (annually)				CI
45	R Review and reclassify information				CIA
INFORMATION CUSTODIAN CONTROLS					
11	R Backup recovery procedures				IA
12	R Basic input data validation				I
16	R Data plausibility and field comparison edits				I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE				C
19	R Encryption/hashing of electronic authentication information				C
20	R Environmental protection measures				IA
21	R Environmental protection measures monitoring				IA
22	R Erase re-writeable media prior to reuse				C
27	R IAM Trust Level 3 for information systems				CI
28	O IAM Trust Level 4 for information systems				CI
33	R Limit access to secure areas				CI
34	R Message integrity				I
39	R Regular backup				IA
52	R Test recovery of backup data				IA
55	R Use disposal method for re-writeable media				C
SE WORKFORCE (INFORMATION USER) CONTROLS					
15	R Confirmation of identity and access rights of requester				C
30	O Label: "NYS CONFIDENTIALITY-HIGH"				C
35	R No confidential information in e-mail subject line				C
41	R Retrieval when printing/faxing (immediate)				C
49	R Secure area				CI
50	R Secure physical media when unattended				CI
51	R Situational awareness during verbal communications				C
53	R Transportation handling controls for paper				C
INFORMATION SECURITY OFFICER (ISO) CONTROLS					
1	R Access approval/removal process (audit)				C
47	R Review security procedures and controls (annually)				CIA

CONFIDENTIALITY (C): HIGH		INTEGRITY (I): HIGH		AVAILABILITY (A): MODERATE	
Glossary X-Ref #	R=Required O=Optional				CIA
STATE ENTITY (SE) CONTROLS					
2	R Access approval/removal process in place				C
9	R Approved electronic storage media and devices				C
10	R Approved storage facility				CI
13	R Chain of custody for physical media				C
17	R Destroy when no longer needed				C
23	R Formal change control procedures for information systems				I
24	R Formal test plans and documented results for information systems				I
29	R Information classification and inventory				CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties				C
38	R Privacy disclaimer on e-mail and fax cover sheets				C
40	R Reproduction authorized by information owner				C
48	R Review system and application security logs				CI
56	R Written approval for Transmission, Transportation and Storage (TTS)				C
INFORMATION OWNER CONTROLS					
5	R Access authorized by information owner (written & cc: exec)				C
6	R Access provided to more than one person				A
44	R Review access lists (annually)				CI
45	R Review and reclassify information				CIA
INFORMATION CUSTODIAN CONTROLS					
11	R Backup recovery procedures				IA
12	R Basic input data validation				I
16	R Data plausibility and field comparison edits				I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE				C
19	R Encryption/hashing of electronic authentication information				C
20	R Environmental protection measures				IA
21	R Environmental protection measures monitoring				IA
22	R Erase re-writeable media prior to reuse				C
27	R IAM Trust Level 3 for information systems				CI
28	O IAM Trust Level 4 for information systems				CI
33	R Limit access to secure areas				CI
34	R Message integrity				I
39	R Regular backup				IA
52	R Test recovery of backup data				IA
55	R Use disposal method for re-writeable media				C
SE WORKFORCE (INFORMATION USER) CONTROLS					
15	R Confirmation of identity and access rights of requester				C
30	O Label: "NYS CONFIDENTIALITY-HIGH"				C
35	R No confidential information in e-mail subject line				C
41	R Retrieval when printing/faxing (immediate)				C
49	R Secure area				CI
50	R Secure physical media when unattended				CI
51	R Situational awareness during verbal communications				C
53	R Transportation handling controls for paper				C
INFORMATION SECURITY OFFICER (ISO) CONTROLS					
1	R Access approval/removal process (audit)				C
47	R Review security procedures and controls (annually)				CIA

CONFIDENTIALITY (C): HIGH		INTEGRITY (I): HIGH	AVAILABILITY (A): HIGH
Glossary	R=Required O=Optional		CIA
X-Ref #			
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan		A
9	R Approved electronic storage media and devices		C
10	R Approved storage facility		CI
13	R Chain of custody for physical media		C
17	R Destroy when no longer needed		C
23	R Formal change control procedures for information systems		I
24	R Formal test plans and documented results for information systems		I
29	R Information classification and inventory		CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties		C
38	R Privacy disclaimer on e-mail and fax cover sheets		C
40	R Reproduction authorized by information owner		C
48	R Review system and application security logs		CI
56	R Written approval for Transmission, Transportation and Storage (TTS)		C
INFORMATION OWNER CONTROLS			
5	R Access authorized by information owner (written & cc: exec)		C
6	R Access provided to more than one person		A
44	R Review access lists (annually)		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
8	R Alternate means of availability		A
11	R Backup recovery procedures		IA
12	R Basic input data validation		I
16	R Data plausibility and field comparison edits		I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE		C
19	R Encryption/hashing of electronic authentication information		C
20	R Environmental protection measures		IA
21	R Environmental protection measures monitoring		IA
22	R Erase re-writeable media prior to reuse		C
27	R IAM Trust Level 3 for information systems		CI
28	O IAM Trust Level 4 for information systems		CI
33	R Limit access to secure areas		CI
34	R Message integrity		I
37	R Off-site backup		A
39	R Regular backup		IA
52	R Test recovery of backup data		IA
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
15	R Confirmation of identity and access rights of requester		C
30	O Label: "NYS CONFIDENTIALITY-HIGH"		C
35	R No confidential information in e-mail subject line		C
41	R Retrieval when printing/faxing (immediate)		C
49	R Secure area		CI
50	R Secure physical media when unattended		CI
51	R Situational awareness during verbal communications		C
53	R Transportation handling controls for paper		C
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
1	R Access approval/removal process (audit)		C
47	R Review security procedures and controls (annually)		CIA

CONFIDENTIALITY CONTROLS	
Glossary X-Ref #	R=Required O=Optional
LOW CONTROLS	
2	R Access approval/removal process in place
3	R Access authorized by information owner
22	R Erase re-writeable media prior to reuse
25	O IAM Trust Level 1 for information systems
29	R Information classification and inventory
31	O Label: "NYS CONFIDENTIALITY-LOW"
38	R Privacy disclaimer on e-mail and fax cover sheets
43	R Review access lists
45	R Review and reclassify information
46	R Review security procedures and controls
54	R Use disposal method for paper or write-once media
55	R Use disposal method for re-writeable media
MODERATE CONTROLS	
4	R Access authorized by information owner (written)
14	R Conceal physical media
15	R Confirmation of identity and access rights of requester
17	R Destroy when no longer needed
26	R IAM Trust Level 2 for information systems
32	O Label: "NYS CONFIDENTIALITY-MODERATE"
42	R Retrieval when printing/faxing (timely)
49	R Secure area
HIGH CONTROLS	
1	R Access approval/removal process (audit)
5	R Access authorized by information owner (written & cc: exec)
9	R Approved electronic storage media and devices
10	R Approved storage facility
13	R Chain of custody for physical media
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE
19	R Encryption/hashing of electronic authentication information
27	R IAM Trust Level 3 for information systems
28	O IAM Trust Level 4 for information systems
30	O Label: "NYS CONFIDENTIALITY-HIGH"
33	R Limit access to secure areas
35	R No confidential information in e-mail subject line
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties
40	R Reproduction authorized by information owner
41	R Retrieval when printing/faxing (immediate)
44	R Review access lists (annually)
47	R Review security procedures and controls (annually)
48	R Review system and application security logs
50	R Secure physical media when unattended
51	R Situational awareness during verbal communications
53	R Transportation handling controls for paper
56	R Written approval for Transmission, Transportation and Storage (TTS)

INTEGRITY CONTROLS	
Glossary X-Ref #	R=Required O=Optional
LOW CONTROLS	
12	R Basic input data validation
25	O IAM Trust Level 1 for information systems
29	R Information classification and inventory
43	R Review access lists
45	R Review and reclassify information
46	R Review security procedures and controls
MODERATE CONTROLS	
11	R Backup recovery procedures
16	R Data plausibility and field comparison edits
20	R Environmental protection measures
23	R Formal change control procedures for information systems
24	R Formal test plans and documented results for information systems
26	R IAM Trust Level 2 for information systems
39	R Regular backup
49	R Secure area
HIGH CONTROLS	
10	R Approved storage facility
21	R Environmental protection measures monitoring
27	R IAM Trust Level 3 for information systems
28	O IAM Trust Level 4 for information systems
33	R Limit access to secure areas
34	R Message integrity
44	R Review access lists (annually)
47	R Review security procedures and controls (annually)
48	R Review system and application security logs
50	R Secure physical media when unattended
52	R Test recovery of backup data

AVAILABILITY CONTROLS	
Glossary	
X-Ref #	R=Required O=Optional
LOW CONTROLS	
29	R Information classification and inventory
45	R Review and reclassify information
46	R Review security procedures and controls
MODERATE CONTROLS	
6	R Access provided to more than one person
11	R Backup recovery procedures
20	R Environmental protection measures
39	R Regular backup
HIGH CONTROLS	
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan
8	R Alternate means of availability
21	R Environmental protection measures monitoring
37	R Off-site backup
47	R Review security procedures and controls (annually)
52	R Test recovery of backup data

Information Classification and Control Appendix E

Glossary of Information Security Controls

Original Publication Date: October 10, 2008
Revision Date: February 7, 2012

Glossary of Information Security Controls
LOW (L), MODERATE (M) and HIGH (H) IMPACT CONTROLS

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION / CLARIFICATION	C I A	CONTROL RATING	SUGGESTED ROLE
1	Access approval/removal process (audit)	R	Authorization	Audit the access approval/removal process at least annually.	C	HIGH	ISO
2	Access approval/removal process in place	R	Authorization	The State Entity must have a formal documented process in place to grant access to it's information assets. Information is provided on either a role-based or need to know/need to do basis. Access is granted for a specific need and is taken away when the need is no longer present.	C	LOW	State Entity
3	Access authorized by information owner	R	Authorization	Responsibility for authorizing access resides solely with the information owner. Users requiring access must follow State Entity's access approval process.	C	LOW	Owner
4	Access authorized by information owner (written)	R	Authorization	The information owner must provide written authorization for access. This does not include normal business processes such as IT having access to files for backup purposes or the travel unit having access to all employee travel documents. This authorization may include a blanket approval for a user or groups of users.	C	MODERATE	Owner
5	Access authorized by information owner (written & cc: exec)	R	Authorization	The information owner must provide written authorization for access with a cc: to executive management. This does not include normal business processes such as IT having access to files for backup purposes or the travel unit having access to all employee travel documents. This authorization may include a blanket approval for a user or groups of users.	C	HIGH	Owner
6	Access provided to more than one person	R	Authorization	Ensure that more than one person has access to the information for business continuity purposes.	A	MODERATE	Owner
7	Address recovery in State Entity Business Continuity/Disaster Recovery Plan	R	Backup	A Business Impact Analysis is conducted to identify priority business processes and the information they depend on. Continuity Plan must include a disaster recovery strategy with the goal to resume normal operations in a reasonable timeframe. Disaster recovery procedures must be up-to-date and periodically tested.	A	HIGH	State Entity
8	Alternate means of availability	R	Backup	Appropriate processes are in place (e.g., redundant hardware, mirroring/replication/shadowing, alternate sites) for data availability.	A	HIGH	Custodian
9	Approved electronic storage media and devices	R	Storage	Electronic storage media and devices must be issued, owned, controlled or approved by the State Entity. This includes media used to record and store data, but not limited to tapes, hard drives, USB flash drives, memory cards/chips, CDs, diskettes.	C	HIGH	State Entity
10	Approved storage facility	R	Storage	Approved storage facilities are Office of Technology (OFT) Data Centers, State Entity physically secured central servers/data center(s), and other facilities as approved in writing by State Entity executive management, upon recommendation of the State Entity ISO. The internal data communication networks of these facilities are included in the approval.	CI	HIGH	State Entity
11	Backup recovery procedures	R	Backup	Written procedures for recovery of electronic information from backup must be defined and tested.	IA	MODERATE	Custodian
12	Basic input data validation	R	System	Incorporate logical checks for electronic information (e.g., valid date checking routine, phone number should not have any letters, validating field lengths before accepting the data).	I	LOW	Custodian
13	Chain of custody for physical media	R	Administrative	Written procedures must be created and implemented to keep track of individual documents, files, devices or media which contain the data and the individuals who have possession of them.	C	HIGH	State Entity
14	Conceal physical media	R	Storage	Conceal paper and/or portable electronic storage media when work area is unoccupied to prevent unintentional disclosure.	C	MODERATE	User

Glossary of Information Security Controls
LOW (L), MODERATE (M) and HIGH (H) IMPACT CONTROLS

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION / CLARIFICATION	C I A	CONTROL RATING	SUGGESTED ROLE
15	Confirmation of identity and access rights of requester	R	Distribution	Before distributing information, verify with information owner that requester has legitimate access rights. In person, verify identity through physical recognition or photo ID. Over phone, verify identity through voice recognition or call back to a known valid number. For courier/e-mail/US postal mail send to the attention of the requester.	C	MODERATE	User
16	Data plausibility and field comparison edits	R	System	As appropriate, include checks to determine that the electronic information entered is reasonable. This is usually an automated process which uses statistics to find unlikely data based on historical information.	I	MODERATE	Custodian
17	Destroy when no longer needed	R	Disposal	Subject to the State Entity's and SARA's record retention and secure disposition requirements, the following must be used: Paper - shredding or incineration Electronic Storage Media - destroy using most appropriate State Entity approved method (e.g., wiping utilities which must have verification, shredding, degaussing). Be aware that some devices (e.g., copiers, printers, fax machines) have hard drives (i.e., image remains on drive). You may need to overwrite storage by copying/sending blank pages. Also, be aware that information may remain in the print spool (i.e., on server if network printer, on local PC if local printer).	C	MODERATE	State Entity
18	Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	R	Distribution Storage	Encryption of electronic information using a State Entity approved encryption methodology is required for transmission (includes email, ftp, etc.), transportation or storage outside of an State Entity approved storage facility. If, due to technical constraints, business limitations, or statutory requirements; a State Entity is unable to implement this control for portable electronic storage media, the following transportation handling controls must be part of a State Entity's compensating controls. This exemption does not apply to laptops, PDA's or USB Flash Drives. Refer to Cyber Security Standard S10-006, Cryptographic Controls. Within office : Hand delivery Outside office : °Hand delivery by State Entity workforce or delivery via courier (e.g., OGS, FedEx, UPS, US Postal Service) °Receipt confirmation °Double-sealed in appropriate secure container, addressed to specific recipient with no special marking on outer container	C	HIGH	Custodian
19	Encryption/hashing of electronic authentication information	R	Distribution Storage	Encryption or hashing is required for electronic information used to authenticate the identity of an individual or process (i.e., PIN, password, passphrase) regardless of where the authentication information is stored, transported or transmitted. This does not include the distribution of a one-time use PIN, password, passphrase, etc. (e.g., administrator forced password change).	C	HIGH	Custodian
20	Environmental protection measures	R	Storage	HVAC, fire suppression, surge protection, uninterrupted power supply (UPS), water protection measures (e.g., master shutoff valves) are in place.	IA	MODERATE	Custodian
21	Environmental protection measures monitoring	R	Storage	Monitor environmental protection measures (i.e., HVAC, fire suppression) for problems and correct as needed.	IA	HIGH	Custodian

Glossary of Information Security Controls
LOW (L), MODERATE (M) and HIGH (H) IMPACT CONTROLS

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION / CLARIFICATION	C I A	CONTROL RATING	SUGGESTED ROLE
22	Erase re-writeable media prior to reuse	R	Distribution	Use a State Entity approved erase method (e.g., wiping utilities which must have verification, degaussing). The reason for this is that it is too difficult to know for certain what class of information currently exists or previously existed on the media. It is possible that data was deleted, but is still recoverable via undelete or forensic tools. Media includes tapes, hard drives, USB flash drives, memory cards/chips, CDs, diskettes, etc..	C	LOW	Custodian
23	Formal change control procedures for information systems	R	Administrative	In the event change to data, applications or system software (e.g., database rollback, source code change) is needed, a formal written record of all changes made must be maintained. For emergency changes, measures must be in place for subsequent review and assessment. If necessary, changes must be resubmitted following the normal change control procedure and the emergency changes removed.	I	MODERATE	State Entity
24	Formal test plans and documented results for information systems	R	Administrative	Plans for testing application software and programs must be devised and documented. This includes: the testing approach, criteria for test completeness, test termination criteria and user acceptance testing and signoff. Result summaries from these tests must be maintained.	I	MODERATE	State Entity
25	IAM Trust Level 1 for information systems	O	Authentication	Refer to NYS Identity and Access Management (IAM): Trust Model. This document defines the processes to establish identities and manage credentials; defines the levels of trust; and provides detailed procedures to map the identity and credential management processes to the various trust levels. Trust Level 1 - little or no confidence in the asserted identity's validity. See the Identity and Access Management: Trust Model at http://www.cio.ny.gov/policy/G07-001/G07-001.pdf for further detail.	CI	LOW	Custodian
26	IAM Trust Level 2 for information systems	R	Authentication	Refer to NYS Identity and Access Management (IAM): Trust Model. This document defines the processes to establish identities and manage credentials; defines the levels of trust; and provides detailed procedures to map the identity and credential management processes to the various trust levels. Trust Level 2 - Confidence exists that the asserted identity is accurate. See the Identity and Access Management: Trust Model at http://www.cio.ny.gov/policy/G07-001/G07-001.pdf for further detail.	CI	MODERATE	Custodian
27	IAM Trust Level 3 for information systems	R	Authentication	Refer to NYS Identity and Access Management (IAM): Trust Model. This document defines the processes to establish identities and manage credentials; defines the levels of trust; and provides detailed procedures to map the identity and credential management processes to the various trust levels. Trust Level 3 - High confidence in the asserted identity's validity. See the Identity and Access Management: Trust Model at http://www.cio.ny.gov/policy/G07-001/G07-001.pdf for further detail.	CI	HIGH	Custodian
28	IAM Trust Level 4 for information systems	O	Authentication	Refer to NYS Identity and Access Management (IAM): Trust Model. This document defines the processes to establish identities and manage credentials; defines the levels of trust; and provides detailed procedures to map the identity and credential management processes to the various trust levels. Trust Level 4 - Very high confidence in the asserted identity's validity. See the Identity and Access Management: Trust Model at http://www.cio.ny.gov/policy/G07-001/G07-001.pdf for further detail.	CI	HIGH	Custodian

Glossary of Information Security Controls
LOW (L), MODERATE (M) and HIGH (H) IMPACT CONTROLS

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION / CLARIFICATION	C I A	CONTROL RATING	SUGGESTED ROLE
29	Information classification and inventory	R	Administrative	1. Classify information assets on an ongoing basis. Information classification must be readily available to all users. 2. Maintain a written or electronic inventory of all information assets. See Section 1. Identification of Information Assets in the Information Classification Manual for further detail.	CIA	LOW	State Entity
30	Label: "NYS CONFIDENTIALITY-HIGH"	O	Labeling	If choosing to label paper or portable electronic storage media, use the label "NYS CONFIDENTIALITY-HIGH". This doesn't replace existing internal labeling structures, but must be included when labeling is used to facilitate the uniform application of controls when information is shared between State Entities. If document is not bound, label each page. Label front and back covers of bound documents.	C	HIGH	User
31	Label: "NYS CONFIDENTIALITY-LOW"	O	Labeling	If choosing to label paper or portable electronic storage media, use the label "NYS CONFIDENTIALITY-LOW". This doesn't replace existing internal labeling structures, but must be included when labeling is used to facilitate the uniform application of controls when information is shared between State Entities.	C	LOW	User
32	Label: "NYS CONFIDENTIALITY-MODERATE"	O	Labeling	If choosing to label paper or portable electronic storage media, use the label "NYS CONFIDENTIALITY-MODERATE". This doesn't replace existing internal labeling structures, but must be included when labeling is used to facilitate the uniform application of controls when information is shared between State Entities.	C	MODERATE	User
33	Limit access to secure areas	R	Authorization	Access is granted to secure areas for a specific need and is taken away when the need is no longer present.	CI	HIGH	Custodian
34	Message integrity	R	Authentication	For electronic data in transit over shared networks (e.g., Internet, NYeNet), integrity checking techniques such as message authentication codes, digital signatures, digitally signed timestamps, and cryptographic hashes, or notarizations must be implemented at the application level. Methods to certify integrity of the data and of the sender must be used when sending data over shared networks with insufficient protections.	I	HIGH	Custodian
35	No confidential information in e-mail subject line	R	Distribution	Confidential information must not be placed in the e-mail subject line, since headers are generally not encrypted.	C	HIGH	User
36	Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	R	Distribution	A formal written agreement with the third party containing requirements for the handling of data must be in place prior to distributing information to them.	C	HIGH	State Entity
37	Off-site backup	R	Storage	Backup copies of portable electronic storage media must be stored at an appropriate secure secondary site approved by the State Entity. Private homes and cars are never appropriate secondary sites.	A	HIGH	Custodian
38	Privacy disclaimer on e-mail and fax cover sheets	R	Distribution	A State Entity approved disclaimer is attached to e-mails and fax cover sheets stating that the contents are intended for the addressed recipient only and must be deleted/destroyed if received in error.	C	LOW	State Entity
39	Regular backup	R	Backup	Information owner defines backup requirements for electronic media in consultation with the custodian. Information custodian backs up data in accordance with these requirements.	IA	MODERATE	Custodian

Glossary of Information Security Controls
LOW (L), MODERATE (M) and HIGH (H) IMPACT CONTROLS

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION / CLARIFICATION	C I A	CONTROL RATING	SUGGESTED ROLE
40	Reproduction authorized by information owner	R	Reproduction	Permission must be obtained (from the information owner) to reproduce information, including voice recordings. This does not include normal business processes such as IT backup of file systems. This authorization may include a blanket approval for a user or groups of users.	C	HIGH	State Entity
41	Retrieval when printing/faxing (immediate)	R	Reproduction	While printing, copying or faxing do not allow shoulder surfing and be aware of those around you. Pick up information immediately.	C	HIGH	User
42	Retrieval when printing/faxing (timely)	R	Reproduction	Pick up copies or printouts as soon as practical.	C	MODERATE	User
43	Review access lists	R	Authorization	Information owner reviews and approves access control lists (i.e., who has access) at a documented interval determined by the State Entity.	CI	LOW	Owner
44	Review access lists (annually)	R	Authorization	Information owner reviews and approves access control lists (i.e., who has access) at a minimum annually.	CI	HIGH	Owner
45	Review and reclassify information	R	Administrative	Information owners are responsible for reviewing and reclassifying (if needed) the information they own at a documented interval determined by the State Entity.	CIA	LOW	Owner
46	Review security procedures and controls	R	Administrative	Review the appropriateness of security procedures and controls at a documented interval determined by the State Entity.	CIA	LOW	ISO
47	Review security procedures and controls (annually)	R	Administrative	Review the appropriateness of security procedures and controls, at a minimum, annually.	CIA	HIGH	ISO
48	Review system and application security logs	R	Authorization	Security logs must be reviewed on a regularly scheduled basis (e.g., daily, weekly, monthly) to monitor required logging as per Cyber Security Standard S10-005. Document that the logs have been reviewed.	CI	HIGH	State Entity
49	Secure area	R	Storage	Store in a secure area when not in physical possession. A secure area is one that is protected by a defined security perimeter, with security barriers and some form of access control (e.g., physical locks, badges, swipe cards, receptionist).	CI	MODERATE	User
50	Secure physical media when unattended	R	Storage	In office, lock paper and/or portable electronic storage media in: safe, office, desk, file cabinet. When traveling, physically secure if unable to keep with you (e.g., store in hotel safe, store in an appropriate locked container, use laptop security cables).	CI	HIGH	User
51	Situational awareness during verbal communications	R	Distribution	Be aware of your surroundings when discussing information, be it in person or using the phone, in order to avoid eavesdropping by unauthorized personnel. Avoid the use of cell phones, two-way radios, or cordless phones as these can be electronically intercepted.	C	HIGH	User
52	Test recovery of backup data	R	Backup	Verify that electronic backup data is recoverable on a bi-annual basis. Recovery objectives are defined and documented. Appropriate resources and personnel are assigned to achieve the objectives.	IA	HIGH	Custodian
53	Transportation handling controls for paper	R	Distribution	Within office (paper): Hand delivery Outside office (paper): °Hand delivery by State Entity workforce or delivery via courier (e.g., OGS, FedEx, UPS, US Postal Service) °Sealed envelope addressed to specific recipient	C	HIGH	User
54	Use disposal method for paper or write-once media	R	Disposal	Use ordinary disposal methods such as discarding in trash or recycling.	C	LOW	User

**Glossary of Information Security Controls
LOW (L), MODERATE (M) and HIGH (H) IMPACT CONTROLS**

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION / CLARIFICATION	C I A	CONTROL RATING	SUGGESTED ROLE
55	Use disposal method for re-writeable media	R	Disposal	<p>For electronic storage media (working or non-working) destroy using the most appropriate State Entity approved disposal method (e.g., wiping utilities which must have verification, shredding, degaussing). The reason for this is that it is too difficult to know for certain what class of information currently exists or previously existed on the media. It is possible that data was deleted, but is still recoverable via undelete or forensic tools. Media includes tapes, hard drives, USB flash drives, memory cards/chips, CDs, diskettes, etc..</p> <p>Be aware that some devices (e.g., copiers, printers, fax machines) have hard drives (i.e., image remains on drive). You may need to overwrite storage by copying/sending blank pages. Also, be aware that information may remain in the print spool (i.e., on server if network printer, on local PC if local printer).</p>	C	LOW	Custodian
56	Written approval for Transmission, Transportation and Storage (TTS)	R	Authorization	<p>State Entity executive management must designate the level of management who can give written approval for the following:</p> <ul style="list-style-type: none"> ° transportation or storage of information outside of an approved storage facility ° transmission outside the State Entity <p>All approvals must be documented by designated management.</p> <p>Requests must include a description of the information, the State Entity information owner, the process of transmitting, transporting or storing the information, the intended use of the information, the location of the information and an end date (if applicable) for the use of the information. Approvals can be granted to functions (e.g., transport of backup tapes to off-site storage site, field auditor case files) eliminating the need for individual requests each time information is stored, transported or transmitted.</p>	C	HIGH	State Entity