ANDREW M. CUOMO
Governor

STATE OF NEW YORK
State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

BRIAN DIGMAN
NYS Chief Information Officer
Director, Office of IT Services

New York State Information Technology Standard	**No:** NYS-S14-003
IT Standard: Information Security Controls	**Effective:** 01/17/2014 **Issued By:** NYS ITS **Standard Owner:** Enterprise Information Security Office

1.0 Purpose and Benefits of the Standard

This standard outlines the baseline information security controls necessary to uniformly protect the confidentiality, integrity and availability of information entrusted to New York State Entities (SEs).

2.0 Enterprise IT Policy/Standard Statement

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of Information Technology Services, the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/policy/glossary.htm.

3.0 Scope

This standard is applicable to SEs, staff and all other affiliates (e.g., contractors, vendors, solution providers), which have access to or manage SE information.

4.0 Information Statement

As per the NYS Information Security Policy, each classification of information must have a set of baseline controls.

Information security control charts corresponding to the impact levels (i.e., low, moderate, and high) and security principles (i.e., confidentiality, integrity, and availability) outlined in the NYS Information Classification Standard are contained in Appendix A. The control charts contain the baseline controls that must be implemented for the information classification achieved by answering the questions in the NYS Information Classification Standard. There are 27 control charts in all; however, information owners, custodians and users must only concern themselves with those control charts that reflect their information's classification.

A SE may add more controls but may not alter or remove the original controls. In addition to the 27 control charts, Appendix A includes one page summaries for all confidentiality controls, all integrity controls and all availability controls. Appendix B: Glossary of Information Security Controls provides further explanation/clarification on each control. The glossary should be used in conjunction with the control charts.

The control charts suggest roles (i.e., SE, Information Owner, Information Custodian, SE Workforce, and Information Security Officer) where a control may be assigned. Based on the structure of the SE's organization, the responsibility of the control may be better suited to another role as determined by the SE.

This standard is meant to be used to determine the information security controls based upon a classification, not the specific method for control implementation.

5.0 Compliance

This standard shall take effect upon publication. The Policy Unit shall review the standard at least once every year to ensure relevancy. The Office may also assess agency compliance with this standard. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber or Legislative entities.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, SEs shall request an exception through the Enterprise Information Security exception process.

6.0 Definitions of Key Terms

Not Applicable

7.0 ITS Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

Standard Owner
Attention: Enterprise Information Security Office
New York State Office of Information Technology Services
State Capitol, ESP, P.O. Box 2062
Albany, NY 12220
Telephone: (518) 242-5200
Facsimile: (518) 322-4976

Questions may also be directed to your ITS Customer Relations Manager at:
Customer.Relations@its.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
http://www.its.ny.gov/tables/technologypolicyindex.htm

8.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
10/10/2008	Original Standard Release (released under the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC))	
01/17/2014	Rebranded for the Office of Information Technology Services; (replaces CSCIC/OCS PS08-001 Information Classification and Control); split into two standards – Information Classification and Information Security Controls	Thomas Smith, Chief Information Security Officer
01/17/2015	Scheduled Standard Review	

9.0 Related Documents

New York State Information Classification Standard

Information Control Charts
Classification Rating Menu

Page #	Classification Rating	Confidentiality	Integrity	Availability
A-1	LLL	Low	Low	Low
A-2	LLM	Low	Low	Moderate
A-3	LLH	Low	Low	High
A-4	LML	Low	Moderate	Low
A-5	LMM	Low	Moderate	Moderate
A-6	LMH	Low	Moderate	High
A-7	LHL	Low	High	Low
A-8	LHM	Low	High	Moderate
A-9	LHH	Low	High	High
A-10	MLL	Moderate	Low	Low
A-11	MLM	Moderate	Low	Moderate
A-12	MLH	Moderate	Low	High
A-13	MML	Moderate	Moderate	Low
A-14	MMM	Moderate	Moderate	Moderate
A-15	MMH	Moderate	Moderate	High
A-16	MHL	Moderate	High	Low
A-17	MHM	Moderate	High	Moderate
A-18	MHH	Moderate	High	High
A-19	HLL	High	Low	Low
A-20	HLM	High	Low	Moderate
A-21	HLH	High	Low	High
A-22	HML	High	Moderate	Low
A-23	HMM	High	Moderate	Moderate
A-24	HMH	High	Moderate	High
A-25	HHL	High	High	Low
A-26	HHM	High	High	Moderate
A-27	HHH	High	High	High
A-28	Confidentiality Controls			
A-29	Integrity Controls			
A-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
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
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
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
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 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
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
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
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
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
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
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 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
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
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
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 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
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
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 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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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 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
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
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
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
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
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
39	R Regular backup
49	R Secure area
	HIGH CONTROLS
10	R Approved storage facility
21	R Environmental protection measures monitoring
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

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 Information Technology Services (ITS) Data Centers, State Entity physically secured central servers/data center(s), and other facilities as approved in writing by State Entity executive management. 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

CIA (C=Confidentiality, I=Integrity, A=Availability)
Need (R=Required, O=Optional)

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. 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

CIA (C=Confidentiality, I=Integrity, A=Availability)
Need (R=Required, O=Optional)

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	Formal change control procedures must be followed in the event of a configuration change (i.e., application, software, hardware). 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
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.	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

CIA (C=Confidentiality, I=Integrity, A=Availability)
Need (R=Required, O=Optional)

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
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
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 analyzed near real-time as per the NYS Security Logging Standard.	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

CIA (C=Confidentiality, I=Integrity, A=Availability)
Need (R=Required, O=Optional)

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
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 Where possible obtain receipt confirmation.	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
55	Use disposal method for re-writeable media	R	Disposal	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.. 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	LOW	Custodian

CIA (C=Confidentiality, I=Integrity, A=Availability)
Need (R=Required, O=Optional)

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION / CLARIFICATION	C I A	CONTROL RATING	SUGGESTED ROLE
56	Written approval for Transmission, Transportation and Storage (TTS)	R	Authorization	State Entity executive management must designate the level of management who can give written approval for the following: ° transportation or storage of information outside of an approved storage facility ° transmission outside the State Entity All approvals must be documented by designated management. 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.	C	HIGH	State Entity