

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

New York State Information Technology Standard	<b>No:</b> NYS-S14-003
IT Standard:	<b>Updated:</b> 03/10/17
Information Security	Issued By: NYS Office of Information Technology Services
Controls	Owner: Enterprise Information Security Office

### 1.0 Purpose and Benefits

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 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. Section 2 of Executive Order No. 117, established January 2002, provides the State Chief Information Officer with 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.

### 3.0 Scope

This standard applies to all SEs, defined as "State Government" entities as defined in Executive Order 117, established January 2002, or "State Agencies" as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any IT resource for which the SE has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. While an SE may adopt a different standard, it must include the requirements set forth in this one.

#### 4.0 Information Statement

As per the <u>NYS Information Security Policy</u>, 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 <a href="NYS Information Classification Standard">NYS Information Classification Standard</a> 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 <a href="NYS Information Classification Standard">NYS Information Classification Standard</a>. 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. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is expected.

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

#### 6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in <a href="http://www.its.ny.gov/glossary">http://www.its.ny.gov/glossary</a>.

NYS-S14-003 Page 2 of 3

#### 7.0 Contact Information

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

Enterprise Information Security Office
Reference: NYS-S14-003
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12242
Telephone: (518) 242-5000

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

Email: EISO@its.ny.gov

### **8.0 Revision History**

This standard shall be subject to periodic review to ensure relevancy.

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
01/16/2015	Standard Review – no changes	Deborah A. Snyder, Deputy Chief Information Security Officer
03/10/2017	Update of Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
05/20/2021	Updated Scope language	Karen Sorady, Chief Information Security Officer

#### 9.0 Related Documents

NYS Classification Standard

NYS-S14-003 Page 3 of 3

### Appendix A: INFORMATION CONTROL CHARTS CLASSIFICATION RATING MENU

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

CONF	IDENTIALITY (C): LOW	INTEGRITY (I): LOW	AVAILABILITY (A LOW	<b>\)</b> :
Glossary X-Ref #	R=Required O=Opt	ional		CIA
STA	ATE ENTITY (SE) CONT	ROLS		
2		noval process in place		С
29	R Information classific	ation and inventory		CIA
38	R Privacy disclaimer of	on e-mail and fax cover sheets		С
	ORMATION OWNER C	ONTROLS		
3	R Access authorized I	by information owner		С
43	R Review access lists			CI
45	R Review and reclass	ify information		CIA
INF	ORMATION CUSTODIA	N CONTROLS		
12	R Basic input data val	lidation		Ι
22	R Erase re-writeable r	media prior to reuse		С
55	R Use disposal metho	d for re-writeable media		С
	•	MATION USER) CONTROLS		
31	O Label: "NYS CONF			С
54	R Use disposal metho	d for paper or write-once media	<u>a</u>	С
INIE	OPMATION SECUDITY	OFFICER (ISO) CONTROLS		
46	R Review security pro			CIA
70	IX IXEVIEW SECURITY PIO	occured and controls		OiA

CON	FIDENTIALITY (C): LOW	INTEGRITY (I): LOW	AVAILABILITY (A MODERATE	A):
Glossary X-Ref #	R=Required O=Opt	ional		CIA
ST	ATE ENTITY (SE) CONT	ROLS		
2	R Access approval/rer	noval process in place		С
29	R Information classific	ation and inventory		CIA
38	R Privacy disclaimer of	on e-mail and fax cover sheets		С
INF	ORMATION OWNER C	ONTROLS		
3	R Access authorized			С
6	R Access provided to			Α
43	R Review access lists			CI
45	R Review and reclass			CIA
INF	ORMATION CUSTODIA	N CONTROLS		
11	R Backup recovery pr	<u>ocedures</u>		IA
12	R Basic input data val	idation		I
20	R Environmental prote	ection measures		IA
22	R Erase re-writeable	media prior to reuse		С
39	R Regular backup			IA
55	R Use disposal metho	d for re-writeable media		С
SF	WORKFORGE (INFORM	MATION USER) CONTROLS		
31	O Label: "NYS CONF	<u>'</u>		С
54		d for paper or write-once media	<u> </u>	С
		OFFICER (ISO) CONTROLS		
46	R Review security pro	cedures and controls		CIA

CONFID	DENTIALITY (C): LOW	INTEGRITY (I): LOW	AVAILABILITY (A): HIGH			
Glossary X-Ref #	R=Required O=Opt	tional	CIA			
ST	STATE ENTITY (SE) CONTROLS					
2	R Access approval/re	moval process in place	С			
7	R Address recovery i	n SE Business Continuity/Disast	er Recovery Plan A			
29	R Information classific	cation and inventory	CIA			
38	R Privacy disclaimer	on e-mail and fax cover sheets	С			
INF	ORMATION OWNER	CONTROLS				
3	R Access authorized	by information owner	С			
6	R Access provided to	more than one person	A			
43	R Review access lists	2	CI			
45	R Review and reclass	sify information	CIA			
INF	 FORMATION CUSTOD	IAN CONTROLS				
8	R Alternate means of		A			
11	R Backup recovery p		IA			
12	R Basic input data va		1			
20	R Environmental prot	ection measures	IA			
21		ection measures monitoring	IA			
22	R Erase re-writeable	media prior to reuse	С			
37	R Off-site backup		A			
39	R Regular backup		IA			
52	R Test recovery of ba	nckup data	IA			
55		od for re-writeable media	С			
	•	RMATION USER) CONTROLS				
31	O Label: "NYS CONF	FIDENTIALITY-LOW"	С			
54	R Use disposal method	od for paper or write-once media	<u>C</u>			
INIE	ORMATION SECURIT	Y OFFICER (ISO) CONTROLS				
47	Ī	ocedures and controls (annually)				
··	The state of the s	see and control (annually)	-   0"1			

CONFIE	DENTIALITY (C): LOW	INTEGRITY (I): MODERATE	AVAILABILITY (A LOW	):
Glossary X-Ref #	R=Required O=Opt	ional		CIA
	ATE ENTITY (SE) CON		<del></del>	
2	R Access approval/rer	noval process in place		С
23	R Formal change con	trol procedures for information	systems	I
24	R Formal test plans a	nd documented results for infor	mation systems	I
29	R Information classific	ation and inventory		CIA
38	R Privacy disclaimer of	on e-mail and fax cover sheets		С
INF	ORMATION OWNER O	CONTROLS		
3	R Access authorized I	oy information owner		С
43	R Review access lists			CI
45	R Review and reclass	ify information		CIA
INF	 FORMATION CUSTODIA	AN CONTROLS		
11	R Backup recovery pr	<u>ocedures</u>		IA
12	R Basic input data val	<u>lidation</u>		_
16	R Data plausibility and	d field comparison edits		1
20	R Environmental prote	ection measures		IA
22	R Erase re-writeable r	media prior to reuse		С
39	R Regular backup			ΙA
55	R Use disposal metho	d for re-writeable media		С
SE	WORKFORCE (INFOR	MATION USER) CONTROLS		
31	O Label: "NYS CONF			С
49	R Secure area			CI
54	R Use disposal metho	d for paper or write-once media	<u>a</u>	С
INIE	ORMATION SECURITY	OFFICER (ISO) CONTROLS		
46	R Review security pro	` '		CIA
10	Trovious doddiny pro	osas.os ana controlo		0.,,

	ENTIALITY (C): LOW	INTEGRITY (I): MODERATE	AVAILABILITY (A	<b>A)</b> :
Glossary X-Ref #	R=Required O			CIA
	TE ENTITY (SE) C			
2		al/removal process in place		С
23		control procedures for inform		l
24		ans and documented results fo	r information systems	I
29		assification and inventory		CIA
38	R Privacy disclai	mer on e-mail and fax cover sh	<u>neets</u>	С
_	RMATION OWN	ER CONTROLS		
3	R Access authori	zed by information owner		С
6	R Access provide	ed to more than one person		Α
43	R Review acces	<u>s lists</u>		CI
45	R Review and re	classify information		CIA
INFO	RMATION CUST	ODIAN CONTROLS		
11	R Backup recove	ery procedures		IA
12	R Basic input da	ta validation		I
16	R Data plausibilit	y and field comparison edits		I
20	R Environmental	protection measures		IA
22	R Erase re-writea	able media prior to reuse		С
39	R Regular backu	<u>ıp</u>		IA
55	R Use disposal r	nethod for re-writeable media		С
SE W	ORKFORCE (IN	FORMATION USER) CONTRO	DLS	
31		ONFIDENTIALITY-LOW"		С
49	R Secure area			CI
54	R Use disposal i	method for paper or write-once	media	С
INFO	RMATION SECU	RITY OFFICER (ISO) CONTR	OLS	
46		y procedures and controls		CIA

CONFID	ENTIALITY (C): LOW	INTEGRITY (I): MODERATE	AVAILABILITY (A HIGH	<b>A)</b> :
Glossary X-Ref #	P-Poquired O-	Ontional		CIA
	R=Required O=	•		CIA
2	· · · · · · · · · · · · · · · · · · ·	al/removal process in place		С
7		ery in SE Business Continuity/Di	saster Recovery Plan	A
23		control procedures for informa		1
24		ns and documented results for i		I
29		ssification and inventory	,	CIA
38		ner on e-mail and fax cover she	<u>ets</u>	С
INF	ORMATION OWN	ER CONTROLS		
3	R Access authorize	red by information owner		С
6	R Access provide	d to more than one person		Α
43	R Review access			CI
45	R Review and red	classify information		CIA
	_	ODIAN CONTROLS		
8	R Alternate mean			Α
11	R Backup recove			IA
12	R Basic input data			<u> </u>
16		and field comparison edits		<u> </u>
20		protection measures		IA
21		protection measures monitoring		IA
22		ole media prior to reuse		C
37	R Off-site backup			Α
39	R Regular backup			IA IA
52 55	R Test recovery of	ethod for re-writeable media		IA C
33	N USE dispusai ii	lethod for re-writeable friedia		
QF.	WORKEORCE (IN	FORMATION USER) CONTRO	ol S	
31		ONFIDENTIALITY-LOW"	1	С
49	R Secure area	J. I. I. L. I. I. L. I. L. VV		CI
54		ethod for paper or write-once m	nedia	C
<u> </u>	CCC GIOPOGGI II			
INF	ORMATION SECU	RITY OFFICER (ISO) CONTRO	OLS	
47		procedures and controls (annu		CIA

CONFIL	DENTIALITY (C): LOW	INTEGRITY (I): HIGH	AVAILABILITY (A	A):
Glossary X-Ref #	P-Poquired 0-0	)ntional		CIA
	R=Required O=C ATE ENTITY (SE) C	•		CIA
2		removal process in place		С
10	R Approved storage			CI
23		control procedures for information	ation systems	I
24		and documented results for	· · · · · · · · · · · · · · · · · · ·	i
29		sification and inventory	THOMPIGATOR OF COMMO	CIA
38		er on e-mail and fax cover she	eets	C
48		and application security logs	<del>, 0.10</del>	CI
	TO TROVIOUS GYOLOTTIC	and approacher escarry rego		<u> </u>
INF	ORMATION OWNER	R CONTROLS		
3	R Access authorize	d by information owner		С
44	R Review access I	sts (annually)		CI
45	R Review and recla	assify information		CIA
		·		
INF	ORMATION CUSTO	DIAN CONTROLS		
11	R Backup recovery	<u>procedures</u>		IA
12	R Basic input data	<u>validation</u>		I
16	R Data plausibility	and field comparison edits		I
20	R Environmental p	rotection measures		IA
21	R Environmental p	rotection measures monitoring		IA
22	R Erase re-writeable	e media prior to reuse		C
33	R Limit access to s	ecure areas		CI
34	R Message integrit	<u>/</u>		I
39	R Regular backup			IA
52	R Test recovery of	backup data		IA
55	R Use disposal me	thod for re-writeable media		С
		ORMATION USER) CONTRO	DLS	
31		NFIDENTIALITY-LOW"		С
49	R Secure area			CI
50		media when unattended		CI
54	R Use disposal me	thod for paper or write-once r	<u>nedia</u>	С
		ITY OFFICER (ISO) CONTR		
47	R Review security	procedures and controls (ann	ually)	CIA

CONFID	ENTIALITY (C): LOW	INTEGRITY (I): HIGH	AVAILABILITY (A): MODERATE	
Glossary				
X-Ref #	R=Required O:		Cl	Α
	ATE ENTITY (SE)			
2		al/removal process in place	C	
10	R Approved stora	<u> </u>	C	:
23		control procedures for informa		
24		ns and documented results for		
29		ssification and inventory	CI	
38		ner on e-mail and fax cover she		
48	R Review system	and application security logs	С	:
INF	ORMATION OWN	FR CONTROLS		
3	T	zed by information owner	l c	,
6		ed to more than one person	A	
44	R Review access		C	
45		classify information	CI	
	TO THOUSAND AND TO	in orritation.		, ,
		ODIAN CONTROLS		
11	R Backup recove		IA	1
12	R Basic input dat		I	
16		and field comparison edits		
20		protection measures	IA	
21		protection measures monitoring		
22		ble media prior to reuse	C	
33	R Limit access to		С	:
34	R Message integ		I	
39	R Regular backu		IA	
52	R Test recovery		IA	
55	R Use disposal n	nethod for re-writeable media	C	<u>;                                    </u>
QF.	WORKFORCE (IN	FORMATION USER) CONTRO	ni s	
31		ONFIDENTIALITY-LOW"	C	•
49	R Secure area	CIVI IDEIVITALITI -LOV	C	
50		al media when unattended	C	
54		nethod for paper or write-once n		
<del></del>	it Use dispusai II	Tetriod for paper of write-once if	Todia O	,
INF	ORMATION SECU	IRITY OFFICER (ISO) CONTRO	OLS	
47		y procedures and controls (annu	î	Α

CONFIDE	ENTIALITY (C): LOW	INTEGRITY (I): HIGH	AVAILABILITY (. HIGH	A):
Glossary X-Ref #	D. Dominod	Outional		CIA
	R=Required O=	•		CIA
2		al/removal process in place		С
7		ery in SE Business Continuity/D	isaster Recovery Plan	A
10	R Approved stora		isaster recovery riam	CI
23		control procedures for informa	ation systems	I
24		ns and documented results for		i
29		ssification and inventory	THE THAT OF THE PARTY OF THE PA	CIA
38		ner on e-mail and fax cover she	eets	C
48		and application security logs	7010	CI
	,			
INF	ORMATION OWN	ER CONTROLS		
3	R Access authoriz	zed by information owner		С
6		d to more than one person		Α
44	R Review access	lists (annually)		CI
45	R Review and red	classify information		CIA
INF	ORMATION CUST	ODIAN CONTROLS		
8	R Alternate mean			Α
11	R Backup recove	ry procedures		IA
12	R Basic input dat			l
16	R Data plausibility	and field comparison edits		I
20	R Environmental	protection measures		IA
21		protection measures monitoring		IA
22		ble media prior to reuse		С
33	R Limit access to			CI
34	R Message integr	<u>rity</u>		l
37	R Off-site backup			Α
39	R Regular backu			IA
52	R Test recovery			IA
55	R Use disposal m	nethod for re-writeable media		С
		FORMATION USER) CONTRO	DLS	
31		ONFIDENTIALITY-LOW"		С
49	R Secure area			CI
50		Il media when unattended		CI
54	R Use disposal m	nethod for paper or write-once r	<u>nedia</u>	С
	_	RITY OFFICER (ISO) CONTR		014
47	R Review security	procedures and controls (ann	ually)	CIA

	ENTIALITY (C): DERATE	INTEGRITY (I): LOW	AVAILABILITY (A LOW	<b>)</b> :
Glossary X-Ref #	R=Required O:	=Optional		CIA
STA	ATE ENTITY (SE)	CONTROLS		
2	R Access approv	al/removal process in place		С
17	R Destroy when	no longer needed		С
29	R Information cla	ssification and inventory		CIA
38	R Privacy disclair	ner on e-mail and fax cover she	ets	С
INF	ORMATION OWN	ER CONTROLS		
4		zed by information owner (writte	en)	С
43	R Review access	s lists		CI
45	R Review and re	classify information		CIA
		ODIAN CONTROLS		
12	R Basic input dat			
22		ble media prior to reuse		С
55	R Use disposal n	nethod for re-writeable media		С
		FORMATION USER) CONTRO	DLS	
14	R Conceal physic			С
15		f identity and access rights of re		С
32		ONFIDENTIALITY-MODERATE	"	С
42		printing/faxing (timely)		С
49	R Secure area			CI
	<u> </u>		_	
		IRITY OFFICER (ISO) CONTRO	OLS	
46	R Review securit	y procedures and controls		CIA

	DENTIALITY (C): ODERATE	INTEGRITY (I): LOW	AVAILABILITY (A): MODERATE
Glossary X-Ref #	D. Domissod O	Ontional	CIA
	R=Required O: ATE ENTITY (SE)	•	CIA
2		al/removal process in place	С
17	R Destroy when		C
29		ssification and inventory	CIA
38		ner on e-mail and fax cover she	eets C
INF	ORMATION OWN	ER CONTROLS	
4		zed by information owner (writte	en) C
6	R Access provide	ed to more than one person	A
43	R Review access	<u>lists</u>	CI
45	R Review and re	classify information	CIA
INF	FORMATION CUST	ODIAN CONTROLS	
11	R Backup recove	ery procedures	IA
12	R Basic input dat	a validation	1
20	R Environmental	protection measures	IA
22	R Erase re-writea	ble media prior to reuse	С
39	R Regular backu	<u>0</u>	IA
55	R Use disposal n	nethod for re-writeable media	С
		FORMATION USER) CONTRO	
14	R Conceal physic		С
15		f identity and access rights of re	
32		ONFIDENTIALITY-MODERATE	
42		printing/faxing (timely)	С
49	R Secure area		CI
		IRITY OFFICER (ISO) CONTRO	
46	K Review securit	y procedures and controls	CIA

	ENTIALITY (C): DDERATE	INTEGRITY (I): LOW	AVAILABILITY (A	A):
Glossary X-Ref #	R=Required O:	=Optional		CIA
STA	ATE ENTITY (SE)	CONTROLS		
2	R Access approv	al/removal process in place		С
7	R Address recove	ery in SE Business Continuity/D	isaster Recovery Plan	Α
17	R Destroy when	no longer needed		С
29	R Information cla	ssification and inventory		CIA
38	R Privacy disclain	ner on e-mail and fax cover she	ets	С
INF	ORMATION OWN	ER CONTROLS		
4	R Access authorize	zed by information owner (writte	en)	С
6	R Access provide	ed to more than one person		Α
43	R Review access	lists		CI
45	R Review and re	classify information		CIA
INF	ORMATION CUST	ODIAN CONTROLS		
8	R Alternate mean	s of availability		Α
11	R Backup recove	ry procedures		IA
12	R Basic input dat	a validation		I
20	R Environmental	protection measures		ΙA
21	R Environmental	protection measures monitoring		ΙA
22	R Erase re-writea	ble media prior to reuse		С
37	R Off-site backup	)		Α
39	R Regular backu	<u>o</u>		ΙA
52	R Test recovery	of backup data		IA
55	R Use disposal m	nethod for re-writeable media		С
SE	WORKFORCE (IN	FORMATION USER) CONTRO	DLS	
14	R Conceal physic	•		С
15	R Confirmation of	f identity and access rights of r	equester_	С
32		ONFIDENTIALITY-MODERATE		С
42	R Retrieval when	printing/faxing (timely)		С
49	R Secure area			CI
INF	ORMATION SECU	IRITY OFFICER (ISO) CONTR	OLS	
47		y procedures and controls (ann		CIA

**AVAILABILITY (A): CONFIDENTIALITY (C):** INTEGRITY (I): MODERATE MODERATE LOW Glossary X-Ref # R=Required O=Optional CIA STATE ENTITY (SE) CONTROLS R Access approval/removal process in place 2 С С 17 R Destroy when no longer needed 23 R Formal change control procedures for information systems I 24 R Formal test plans and documented results for information systems ı 29 CIA R Information classification and inventory

23	13 Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	С
INI	FORMATION OWNER CONTROLS	
4	R Access authorized by information owner (written)	С
43	R Review access lists	CI
45	R Review and reclassify information	CIA
IN	FORMATION CUSTODIAN CONTROLS	•
11	R Backup recovery procedures	IA
12	R Basic input data validation	- 1
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
22	R Erase re-writeable media prior to reuse	С
39	R Regular backup	IA
55	R Use disposal method for re-writeable media	С
0.5	TWODE CORE (INFORMATION LIGER) CONTROL O	
14	R Conceal physical media	С
15	R Confirmation of identity and access rights of requester	C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	С
42	R Retrieval when printing/faxing (timely)	С
49	R Secure area	CI
46	R Review security procedures and controls	CIA

	ENTIALITY (C): DERATE	INTEGRITY (I): MODERATE	AVAILABILITY (A MODERATE	A):
Glossary X-Ref #	R=Required O:	•		CIA
	TE ENTITY (SE) (			
2		al/removal process in place		С
17	R Destroy when			С
23		control procedures for information		I
24	R Formal test pla	ns and documented results for	information systems	I
29		ssification and inventory		CIA
38	R Privacy disclair	ner on e-mail and fax cover sh	<u>eets</u>	С
INFO	RMATION OWN	ER CONTROLS		
4		zed by information owner (writt	<u>:en)</u>	С
6	R Access provide	d to more than one person		Α
43	R Review access	s lists		CI
45	R Review and red	classify information		CIA
INFO	DRMATION CUST	ODIAN CONTROLS		
11	R Backup recove	ry procedures		IA
12	R Basic input dat	a validation		I
16	R Data plausibility	and field comparison edits		I
20	R Environmental	protection measures		ΙA
22	R Erase re-writea	ble media prior to reuse		С
39	R Regular backu	<u>p</u>		IA
55	R Use disposal n	nethod for re-writeable media		С
SE V	VORKFORCE (IN	FORMATION USER) CONTRO	DLS	
14	R Conceal physic	al media		С
15	R Confirmation o	f identity and access rights of	<u>requester</u>	С
32	O Label: "NYS C	ONFIDENTIALITY-MODERATE	="	С
42	R Retrieval when	printing/faxing (timely)		С
49	R Secure area			CI
INFO	RMATION SECU	RITY OFFICER (ISO) CONTR	OLS	
46		procedures and controls		CIA
	1			1

	ENTIALITY (C): DDERATE	INTEGRITY (I): MODERATE	AVAILABILITY (A	A):
Glossary	_			_
X-Ref #	R=Required O=	•		CIA
	TE ENTITY (SE)			
7		I/removal process in place	anatar Banayary Dlan	C A
17		ry in SE Business Continuity/Di	saster Recovery Plan	C
23	R Destroy when n	control procedures for information	tion systems	
24		is and documented results for i		
29		sification and inventory	inionnation systems	CIA
38		er on e-mail and fax cover she	acte	C
30	IX I IIVacy discialii	er on e-mail and tax cover she		
INF	ORMATION OWN	ER CONTROLS		
4		ed by information owner (writte	en)	С
6		to more than one person		A
43	R Review access			CI
45	R Review and rec			CIA
INF	ORMATION CUST	ODIAN CONTROLS		
8	R Alternate means			Α
11	R Backup recover	y procedures		IA
12	R Basic input data			I
16		and field comparison edits		I
20		protection measures		IA
21		protection measures monitoring		IA
22		ole media prior to reuse		С
37	R Off-site backup			Α
39	R Regular backup			IA
52	R Test recovery of			IA
55	R Use disposal m	ethod for re-writeable media		С
<b>AF</b>	MODIFED OF (THE		N 0	
	· · · · · · · · · · · · · · · · · · ·	FORMATION USER) CONTRO	JL5	
14	R Conceal physics		n au La atau	C
15 32		identity and access rights of reDNFIDENTIALITY-MODERATE		C
42		printing/faxing (timely)	_	C
49	R Secure area	printing/raxing (timely)		CI
<del>- 1</del> 3	it Occure area			<u> </u>
INF	ORMATION SECU	RITY OFFICER (ISO) CONTR	OLS	
47		procedures and controls (annu		CIA
	TITLE SOUTH	, see a see	11.	

Glossary X-Ref # R=Required O=Optional STATE ENTITY (SE) CONTROLS  2 R Access approval/removal process in place C10 R Approved storage facility C17 R Destroy when no longer needed C23 R Formal change control procedures for information systems C24 R Formal test plans and documented results for information systems C29 R Information classification and inventory C29 R Information classification and inventory C38 R Privacy disclaimer on e-mail and fax cover sheets C48 R Review system and application security logs C1  INFORMATION OWNER CONTROLS  4 R Access authorized by information owner (written) C44 R Review access lists (annually) C5 R Review and reclassify information C6 R  INFORMATION CUSTODIAN CONTROLS  11 R Backup recovery procedures 11 R Backup recovery procedures 12 R Basic input data validation 13 R Environmental protection measures 14 R Environmental protection measures 15 R Environmental protection measures 16 R Data plausibility and field comparison edits 17 R Environmental protection measures 18 C R Environmental protection measures 19 R Environmental protection measures 20 R Environmental protection measures 21 R Environmental protection measures 22 R Erase re-writeable media prior to reuse 23 R R Require backup 24 R Residen backup 25 R Test recovery of backup data 26 R Test recovery of backup data 27 R Environmental protection users indits of requester 28 R Great recovery of backup data 29 R Regular backup 20 R Environmental protection users indits of requester 29 R Test recovery of backup data 29 R Regular backup 20 R Regular backup 21 R R Review descersing media when unattended 20 R R Review security procedures and controls (annually) 30 R R Require backup R R Review security procedures and controls (annually) 31 R R Review security procedures and controls (annually) 32 R Review security procedures and controls (annually) 33 R R Review security procedures and controls (annually) 34 R Review security procedures and controls (annually)		DENTIALITY (C): DDERATE	INTEGRITY (I): HIGH	AVAILABILITY (A LOW	A):
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 CI  38 R Privacy disclaimer on e-mail and fax cover sheets CA  48 R Review system and application security logs CI  INFORMATION OWNER CONTROLS  4 R Access authorized by information owner (written) CI  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 IA  22 R Erase re-writeable media prior to reuse C  33 R Limit access to secure areas CI  34 R Message integrity IA  55 R Use disposal method for re-writeable media C  SE WORKFORCE (INFORMATION USER) CONTROLS  INFORMATION SECURITY OFFICER (ISO) CONTROLS		P-Poquired O-	Ontional		CIA
2 R Access approval/removal process in place 10 R Approved storage facility 17 R Destroy when no longer needed C1 18 R Formal change control procedures for information systems C2 R Formal change control procedures for information systems C3 R Formal test plans and documented results for information systems C4 R Formal test plans and documented results for information systems C5 R Information classification and inventory C6 R Review cystem and application security logs C7 R Review system and application security logs C8 R Review system and application security logs C9 R Review access lists (annually) C9 R Review access lists (annually) C9 R Review and reclassify information owner (written) C9 R Review and reclassify information C9 R Basic input data validation C9 R Basic input data validation C9 R Basic input data validation C9 R Environmental protection measures C9 R Erase re-writeable media prior to reuse C9 C1 C9 R Test recovery of backup data C9 R Test recover		<u> </u>	•		CIA
10 R Approved storage facility 17 R Destroy when no longer needed C 23 R Formal change control procedures for information systems 1 24 R Formal test plans and documented results for information systems 1 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 A44 R Review access lists (annually) CIA 45 R Review and reclassify information CIA  INFORMATION CUSTODIAN CONTROLS 11 R Backup recovery procedures 12 R Basic input data validation 14 R Data plausibility and field comparison edits 15 R Data plausibility and field comparison edits 16 R Data plausibility and field comparison edits 17 R Environmental protection measures 18 IA 21 R Environmental protection measures 19 IA 21 R Environmental protection measures C R Erase re-writeable media prior to reuse C C R Erase re-writeable media prior to reuse C C C C C C C C C C C C C C C C C C C					С
17 R Destroy when no longer needed 23 R Formal change control procedures for information systems 24 R Formal test plans and documented results for information systems 29 R Information classification and inventory 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 A R Review access lists (annually) C CI 45 R Review and reclassify information C CIA  INFORMATION CUSTODIAN CONTROLS  11 R Backup recovery procedures 12 R Basic input data validation 13 R Environmental protection measures 14 R Environmental protection measures 15 R Erase re-writeable media prior to reuse C CI 33 R Limit access to secure areas C CI 34 R Message integrity J R Regular backup IS R Confirmation of identity and access rights of requester C CI 35 R Confirmation of identity and access rights of requester C CI C R Retrieval when printing/faxing (timely) C CI C C	10				
23   R Formal change control procedures for information systems   1					С
29 R Information classification and inventory  38 R Privacy disclaimer on e-mail and fax cover sheets  C A R Review system and application security logs  CI  INFORMATION OWNER CONTROLS  4 R Access authorized by information owner (written)  C A R Review access lists (annually)  CI  45 R Review and reclassify information  CIA  INFORMATION CUSTODIAN CONTROLS  11 R Backup recovery procedures  12 R Basic input data validation  16 R Data plausibility and field comparison edits  17 R Environmental protection measures  18 A 21 R Environmental protection measures monitoring  20 R Environmental protection measures monitoring  10 A 22 R Erase re-writeable media prior to reuse  C C 33 R Limit access to secure areas  CI A R Message integrity  I A S R Regular backup  52 R Test recovery of backup data  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 C 32 O Label: "NYS CONFIDENTIALITY-MODERATE"  C C C INFORMATION SECURITY OFFICER (ISO) CONTROLS	23			tion systems	I
38 R Privacy disclaimer on e-mail and fax cover sheets  48 R Review system and application security logs  CI  INFORMATION OWNER CONTROLS  4 R Access authorized by information owner (written)  CI  44 R Review access lists (annually)  CI  45 R Review and reclassify information  CIA  INFORMATION CUSTODIAN CONTROLS  11 R Backup recovery procedures  12 R Basic input data validation  16 R Data plausibility and field comparison edits  1 R Environmental protection measures  1A  21 R Environmental protection measures monitoring  IA  22 R Erase re-writeable media prior to reuse  CI  33 R Limit access to secure areas  CI  34 R Message integrity  I A  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 C  42 R Retrieval when printing/faxing (timely)  C C  INFORMATION SECURITY OFFICER (ISO) CONTROLS	24				I
INFORMATION OWNER CONTROLS   A R Access authorized by information owner (written)   C	29	R Information class	ssification and inventory		CIA
INFORMATION OWNER CONTROLS  4 R Access authorized by information owner (written)  CI  44 R Review access lists (annually)  CI  45 R Review and reclassify information  CIA  INFORMATION CUSTODIAN CONTROLS  11 R Backup recovery procedures  12 R Basic input data validation  I R Backup recovery procedures  IA 12 R Basic input data validation  I R Backup recovery procedures  IA 12 R Environmental protection measures  IA 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 INFORMATION SECURITY OFFICER (ISO) CONTROLS	38	R Privacy disclain	ner on e-mail and fax cover she	<u>ets</u>	С
4 R Access authorized by information owner (written) C1 44 R Review access lists (annually) C1 45 R Review and reclassify information C1A  INFORMATION CUSTODIAN CONTROLS  11 R Backup recovery procedures 12 R Basic input data validation I 16 R Data plausibility and field comparison edits I 20 R Environmental protection measures I A 21 R Environmental protection measures monitoring I A 22 R Erase re-writeable media prior to reuse C C 33 R Limit access to secure areas C1 34 R Message integrity I A 52 R Test recovery of backup data 55 R Use disposal method for re-writeable media C C  SE WORKFORCE (INFORMATION USER) CONTROLS 15 R Confirmation of identity and access rights of requester C C 42 R Retrieval when printing/faxing (timely) C C 49 R Secure area C1 INFORMATION SECURITY OFFICER (ISO) CONTROLS	48	R Review system	and application security logs		CI
4 R Access authorized by information owner (written) C1 44 R Review access lists (annually) C1 45 R Review and reclassify information C1A  INFORMATION CUSTODIAN CONTROLS  11 R Backup recovery procedures 12 R Basic input data validation I 6 R Data plausibility and field comparison edits I 1 20 R Environmental protection measures I A 21 R Environmental protection measures monitoring I A 22 R Erase re-writeable media prior to reuse C C 33 R Limit access to secure areas C1 34 R Message integrity I 1 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 C 42 R Retrieval when printing/faxing (timely) C C 49 R Secure area C1 INFORMATION SECURITY OFFICER (ISO) CONTROLS					
44 R Review access lists (annually)  CI  45 R Review and reclassify information  CIA  INFORMATION CUSTODIAN CONTROLS  11 R Backup recovery procedures  12 R Basic input data validation  16 R Data plausibility and field comparison edits  1 R Environmental protection measures  1 R Environmental protection measures  21 R Environmental protection measures monitoring  1 A  22 R Erase re-writeable media prior to reuse  C C  33 R Limit access to secure areas  CI  34 R Message integrity  I A  55 R Test recovery of backup data  55 R Use disposal method for re-writeable media  C C  SE WORKFORCE (INFORMATION USER) CONTROLS  15 R Confirmation of identity and access rights of requester  C C  42 R Retrieval when printing/faxing (timely)  C C  49 R Secure area  CI  INFORMATION SECURITY OFFICER (ISO) CONTROLS					
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 IA 21 R Environmental protection measures 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 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 42 R Retrieval when printing/faxing (timely) C 49 R Secure area CI INFORMATION SECURITY OFFICER (ISO) CONTROLS			· · · · · · · · · · · · · · · · · · ·	<u>en)</u>	
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 55 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			<u> </u>		
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	45	R Review and red	classify information		CIA
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					
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		T			
16 R Data plausibility and field comparison edits 1 20 R Environmental protection measures 1 IA 21 R Environmental protection measures monitoring 1 IA 22 R Erase re-writeable media prior to reuse 23 R Limit access to secure areas 24 C C C C C C C C C C C C C C C C C C C					IA
20 R Environmental protection measures  21 R Environmental protection measures monitoring  22 R Erase re-writeable media prior to reuse  33 R Limit access to secure areas  CI  34 R Message integrity  I 39 R Regular backup  52 R Test recovery of backup data  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  32 O Label: "NYS CONFIDENTIALITY-MODERATE"  C 42 R Retrieval when printing/faxing (timely)  49 R Secure area  CI  INFORMATION SECURITY OFFICER (ISO) CONTROLS					<u> </u>
21 R Environmental protection measures monitoring  22 R Erase re-writeable media prior to reuse  C C  33 R Limit access to secure areas  CI  34 R Message integrity  I 39 R Regular backup  52 R Test recovery of backup data  55 R Use disposal method for re-writeable media  C C  SE WORKFORCE (INFORMATION USER) CONTROLS  15 R Confirmation of identity and access rights of requester  32 O Label: "NYS CONFIDENTIALITY-MODERATE"  C C  42 R Retrieval when printing/faxing (timely)  C C  INFORMATION SECURITY OFFICER (ISO) CONTROLS					<u> </u>
22 R Erase re-writeable media prior to reuse  33 R Limit access to secure areas  CI  34 R Message integrity  I 39 R Regular backup  52 R Test recovery of backup data  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  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					
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					
34 R Message integrity 39 R Regular backup 52 R Test recovery of backup data 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 INFORMATION SECURITY OFFICER (ISO) CONTROLS					
39 R Regular backup 52 R Test recovery of backup data 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 INFORMATION SECURITY OFFICER (ISO) CONTROLS		<del></del>			CI
52 R Test recovery of backup data 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 INFORMATION SECURITY OFFICER (ISO) CONTROLS					
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					
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	_				
15 R Confirmation of identity and access rights of requester 32 O Label: "NYS CONFIDENTIALITY-MODERATE" C 42 R Retrieval when printing/faxing (timely) 49 R Secure area CI 50 R Secure physical media when unattended CI INFORMATION SECURITY OFFICER (ISO) CONTROLS	55	R Use disposal m	ethod for re-writeable media		C
15 R Confirmation of identity and access rights of requester 32 O Label: "NYS CONFIDENTIALITY-MODERATE" C 42 R Retrieval when printing/faxing (timely) 49 R Secure area CI 50 R Secure physical media when unattended CI INFORMATION SECURITY OFFICER (ISO) CONTROLS	C.F.	WORKEOBCE (IN	FORMATION LISERY CONTRO	N 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					
42 R Retrieval when printing/faxing (timely) 49 R Secure area 50 R Secure physical media when unattended CI INFORMATION SECURITY OFFICER (ISO) CONTROLS			, , , , , , , , , , , , , , , , , , , ,		
49 R Secure area CI 50 R Secure physical media when unattended CI  INFORMATION SECURITY OFFICER (ISO) CONTROLS		+			
50 R Secure physical media when unattended CI INFORMATION SECURITY OFFICER (ISO) CONTROLS			printing/raxing (timely)		_
INFORMATION SECURITY OFFICER (ISO) CONTROLS			I media when unattended		
	30	ix Occure priyalca	i media when dhallended		Oi
	INF	ORMATION SECU	RITY OFFICER (ISO) CONTRO	OLS	
It items document production and controlle (armadily)					CIA
,	'' <u>'</u>	T. T. C. T. S. T. C.	p. 13044. Co a.i.a comicio (aline		<u> </u>

	ENTIALITY (C): DDERATE	INTEGRITY (I): HIGH	AVAILABILITY ( MODERATE	A):
Glossary X-Ref #	R=Required O=	-Ontional		CIA
	ATE ENTITY (SE)	•		O.//
2		al/removal process in place		С
10	R Approved stora	ge facility		CI
17	R Destroy when i	no longer needed		С
23		control procedures for informa	tion systems	I
24	R Formal test pla	ns and documented results for	information systems	I
29	R Information cla	ssification and inventory		CIA
38	R Privacy disclain	ner on e-mail and fax cover she	<u>eets</u>	С
48	R Review system	and application security logs		CI
	ORMATION OWN			
4	R Access authorize	zed by information owner (writte	<u>en)</u>	С
6		d to more than one person		Α
44	R Review access	lists (annually)		CI
45	R Review and red	classify information		CIA
		FODIAN CONTROLS		1
11	R Backup recove			IA
12	R Basic input data			l
16		and field comparison edits		I
20	Time to the second seco	protection measures		IA
21		protection measures monitoring		IA
22		ble media prior to reuse		С
33	R Limit access to			CI
34	R Message integ			l
39	R Regular backu			IA
52	R Test recovery			IA
55	R Use disposal m	ethod for re-writeable media		С
<b>0</b> =	WODI/FORGE (III	FORMATION HOERY CONTRA	21.0	
		FORMATION USER) CONTRO		
15		identity and access rights of r		C
32		ONFIDENTIALITY-MODERATE	<u></u>	С
42		printing/faxing (timely)		С
49	R Secure area	Luca adia subsers sussetti si tis t		CI
50	K Secure physica	I media when unattended		CI
INIT	ODMATION CEC	IDITY OFFICER (ISO) CONTR	OI C	
	T	JRITY OFFICER (ISO) CONTR		CIA
47	K Keview Security	procedures and controls (ann	ualiy)	CIA

	DENTIALITY (C): MODERATE	INTEGRITY (I): HIGH	AVAILABILITY ( HIGH	(A):
Glossary X-Ref #	R=Required O=O	ptional		CIA
	ATE ENTITY (SE) CO			
2		removal process in place		С
7		y in SE Business Continuity/Disa	aster Recovery Plan	Α
10	R Approved storag		•	CI
17	R Destroy when no			С
23	R Formal change c	ontrol procedures for informatio	n systems	I
24	R Formal test plans	and documented results for inf	ormation systems	I
29	R Information class	ification and inventory	-	CIA
38	R Privacy disclaime	r on e-mail and fax cover sheet	<u>S</u>	С
48	R Review system a	nd application security logs		CI
INI	FORMATION OWNER	CONTROLS		
4	R Access authorize	ed by information owner (written)		С
6	R Access provided	to more than one person		Α
44	R Review access li	sts (annually)		CI
45	R Review and recla	assify information		CIA
INI	FORMATION CUSTO	DIAN CONTROLS		
8	R Alternate means	of availability		Α
11	R Backup recovery	<u>procedures</u>		IA
12	R Basic input data	<u>validation</u>		I
16		and field comparison edits		I
20	R Environmental pr	otection measures		IA
21	R Environmental pr	otection measures monitoring		IA
22	R Erase re-writeab	le media prior to reuse		С
33	R Limit access to s	ecure areas		CI
34	R Message integrit	<u>Y</u>		
37	R Off-site backup			Α
39	R Regular backup			IA
52	R Test recovery of	<u> </u>		IA
55	R Use disposal me	thod for re-writeable media		С
		DRMATION USER) CONTROLS		
15	-	identity and access rights of req	<u>uester</u>	С
32		NFIDENTIALITY-MODERATE"		С
42		rinting/faxing (timely)		С
49	R Secure area			CI
50	R Secure physical	media when unattended		CI
INI	FORMATION SECURI	TY OFFICER (ISO) CONTROL	S	
47	R Review security	procedures and controls (annual	ly)	CIA

CONFID	ENTIALITY (C): HIGH	INTEGRITY (I): LOW	AVAILABILITY (A) LOW	:
Glossary X-Ref #	R=Required O	=Optional		CIA
STA	TE ENTITY (SE)	CONTROLS		
2	R Access approv	al/removal process in place		С
9	R Approved elec	tronic storage media and devic	es	С
10	R Approved stora	age facility		CI
13	R Chain of custo	dy for physical media		С
17	R Destroy when	no longer needed		С
29	R Information cla	assification and inventory		CIA
36	R Non-Disclosure	e Agreement (NDA), Acceptable	e Use Policy,	С
38	R Privacy disclair	<u>mer on e-mail and fax cover sh</u>	eets	С
40	R Reproduction	authorized by information owne	r	С
48	R Review system	n and application security logs		CI
56	R Written approv	al for Transmission, Transporta	ation and Storage	С
	ORMATION OWN			
5		ized by information owner (write	ten & cc: exec)	С
44	R Review access			CI
45	R Review and re	classify information		CIA
		ODIAN CONTROLS		_
12	R Basic input da		(	<u> </u>
18		Transmission/ Transportation/		C
19		hing of electronic authenticatio	n information	С
22		able media prior to reuse		С
33	R Limit access to			CI
55	R Use disposal r	method for re-writeable media		С
05.	WORKEODOE (IN	FORMATION LIGERY CONTRA	21.0	
		FORMATION USER) CONTRO		
15		of identity and access rights of	requester	C
30	1	ONFIDENTIALITY-HIGH		C
35		information in e-mail subject	IIIE	С
41		n printing/faxing (immediate)		C
49	R Secure area	al modia when unattended		CI
50 51		al media when unattended	ications	CI C
51 53		areness during verbal commun	ICALIUI 15	C
<u> </u>	n Hansportation	handling controls for paper		U
INIE	DEMATION SECTION	RITY OFFICER (ISO) CONTR	OI S	
1		val/removal process (audit)		С
47		y procedures and controls (ann	nually)	CIA
41	IIV IVENIEM SECULI	y procedures and controls (and	iually <i>j</i>	OΙΛ

CONFIDE	ENTIALITY (C): HIGH	INTEGRITY (I): LOW	AVAILABILITY (A) MODERATE	:
Glossary X-				
Ref#	R=Required O=O			CIA
STAT	TE ENTITY (SE) CON	TROLS		
2	R Access approval/	removal process in place		С
9	R Approved electro	nic storage media and devices		С
10	R Approved storage	e facility		CI
13	R Chain of custody	for physical media		С
17	R Destroy when no	<u>longer needed</u>		С
29	R Information class	fication and inventory		CIA
36	R Non-Disclosure A	greement (NDA), Acceptable Use Po	licy, Memorandum of	С
38	R Privacy disclaime	ron e-mail and fax cover sheets		С
40	R Reproduction aut	norized by information owner		С
48	R Review system ar	nd application security logs		CI
56	R Written approval t	or Transmission, Transportation and	Storage (TTS)	С
INFO	RMATION OWNER	CONTROLS		
5	R Access authorize	d by information owner (written & cc:	exec)	С
6	R Access provided	to more than one person		Α
44	R Review access lis	ts (annually)		CI
45	R Review and reclas	ssify information		CIA
INFO	RMATION CUSTOD	AN CONTROLS	•	
11	R Backup recovery	<u>procedures</u>		ΙA
12	R Basic input data v	<u>alidation</u>		I
18	R Encryption for Tra	nsmission/ Transportation/ Storage	(TTS) Outside the SE	С
19	R Encryption/hashir	ng of electronic authentication informa	<u>ation</u>	С
20	R Environmental pro	otection measures		IA
22	R Erase re-writeable	e media prior to reuse		С
33	R Limit access to se	ecure areas		CI
39	R Regular backup			IA
55	R Use disposal met	hod for re-writeable media		С
SEW		MATION USER) CONTROLS		
15	R Confirmation of ic	lentity and access rights of requeste	<u>r</u>	С
30	O Label: "NYS CON	FIDENTIALITY-HIGH"		С
35		formation in e-mail subject line		С
41	R Retrieval when pr	inting/faxing (immediate)		С
49	R Secure area			CI
50	R Secure physical n	nedia when unattended		CI
51		ness during verbal communications		С
53	R Transportation ha	ndling controls for paper		С
INFO	RMATION SECURIT	Y OFFICER (ISO) CONTROLS		
1	R Access approval/	removal process (audit)		С
47	R Review security p	rocedures and controls (annually)		CIA

CONFI	DENTIALITY (C): HIGH	INTEGRITY (I): LOW	AVAILABILITY (A HIGH	):
Glossary				
X-Ref #	R=Required O=Op			CIA
	ATE ENTITY (SE) CO			
2	R Access approval/r	emoval process in place		С
7		in SE Business Continuity/Disaste	er Recovery Plan	Α
9		nic storage media and devices		С
10	R Approved storage			CI
13	R Chain of custody t			С
17	R Destroy when no			С
29		ication and inventory	D. II. M	CIA
36		greement (NDA), Acceptable Use	Policy, Memorandum	С
38		on e-mail and fax cover sheets		С
40		norized by information owner		C
48		ad application security logs		CI
56	R Written approval f	or Transmission, Transportation a	and Storage (TTS)	С
	<b>FORMATION OWNER</b>			
5	R Access authorized	d by information owner (written & o	cc: exec)	С
6	R Access provided t	o more than one person		Α
44	R Review access lis	ts (annually)		CI
45	R Review and reclas	ssify information		CIA
INF	FORMATION CUSTO	DIAN CONTROLS		
8	R Alternate means of			Α
11	R Backup recovery			ÍΑ
12	R Basic input data v			I
18		Insmission/ Transportation/ Stora	ge (TTS) Outside the SE	С
19		g of electronic authentication info		С
20	R Environmental pro			IΑ
21	R Environmental pro	otection measures monitoring		IA
22	R Erase re-writeable	e media prior to reuse		С
33	R Limit access to se	<u>cure areas</u>		CI
37	R Off-site backup			Α
39	R Regular backup			ΙA
52	R Test recovery of b	ackup data		IA
55	R Use disposal meth	nod for re-writeable media		С
QE.	WORKFORCE (INEC	DRMATION USER) CONTROLS		
15		dentity and access rights of reques	ster	С
30	O Label: "NVS CON	FIDENTIALITY-HIGH"	<u>otor</u>	C
35		formation in e-mail subject line		C
41		inting/faxing (immediate)		C
49	R Secure area	ming, raking (ininibalato)		CI
50		nedia when unattended		CI
51		ness during verbal communication	S	C
53		ndling controls for paper		Č
				-
		TY OFFICER (ISO) CONTROLS		
1		emoval process (audit)		C
47	K Review security p	rocedures and controls (annually)		CIA

CONF	IDENTIALITY (C): HIGH	INTEGRITY (I): MODERATE	AVAILABILITY (A): LOW	
Glossary X-Ref #	R=Required O=Opt	tional	CIA	
	ATE ENTITY (SE) CON		<u> </u>	
2		emoval process in place	С	
9		ic storage media and devices	C	
10	R Approved storage	<u> </u>	CI	
13	R Chain of custody for		С	
17	R Destroy when no lo	onger needed	С	
23	R Formal change cor	ntrol procedures for information systematics	ems I	
24	R Formal test plans a	and documented results for information	on systems I	
29				
36				
		or similar device for third-parties		
38		on e-mail and fax cover sheets	С	
40		orized by information owner	C	
48		d application security logs	Cl	
56	R Written approval for	or Transmission, Transportation and S	Storage (TTS) C	
INI	FORMATION OWNER (	CONTROL		
	FORMATION OWNER (		voo)	
5		by information owner (written & cc: e		
44	R Review access list		CI	
45	R Review and reclass	<u>siry information</u>	CIA	
IN	FORMATION CUSTODI	AN CONTROLS		
11	R Backup recovery p		IA IA	
12	R Basic input data va			
16		d field comparison edits	1	
18		smission/ Transportation/ Storage (	ITS) Outside the SE C	
19		of electronic authentication informat		
20	R Environmental prof		IA	
22	R Erase re-writeable	media prior to reuse	С	
33	R Limit access to sec	cure areas	CI	
39	R Regular backup		IA	
55	R Use disposal meth	od for re-writeable media	С	
		RMATION USER) CONTROLS		
15		entity and access rights of requester	C	
30	O Label: "NYS CONF		C	
35		ormation in e-mail subject line	С	
41		ting/faxing (immediate)	C	
49	R Secure area	P. 1. (C. 1.1.)	CI	
50	R Secure physical m		CI	
51		ess during verbal communications	C	
53	K Transportation han	dling controls for paper_	C	
IN	FORMATION SECURIT	Y OFFICER (ISO) CONTROLS		
1	R Access approval/re		C	
47		ocedures and controls (annually)	CIA	
<u> </u>	IN INGVIEW SECURITY PR	occurres and controls (annually)	L CIA	

CONFID	ENTIALITY (C): HIGH	INTEGRITY (I): MODERATE	AVAILABILITY (A): MODERATE				
Glossary							
X-Ref #	R=Required O=O	ptional		CIA			
STA	TE ENTITY (SE) CO						
2		removal process in place		С			
9		nic storage media and devices		С			
10	R Approved storage			CI			
13	R Chain of custody			С			
17	R Destroy when no						
23							
24	29 R Information classification and inventory						
		Agreement (NDA), Acceptable Usi	a Daliay Mamarandum	CIA C			
36 38		r on e-mail and fax cover sheets	e Policy, Memorandum	C			
40		horized by information owner		C			
48		nd application security logs		CI			
56		for Transmission, Transportation	and Storage (TTS)	C			
30	N WITHER Approval	TOT TRAITSTILLSSION, TRAITSPORTATION	and Storage (113)	C			
INFO	DRMATION OWNER	R CONTROLS					
5		d by information owner (written &	cc. exec)	С			
6		to more than one person	<u> </u>	Ā			
44	R Review access lis			CI			
45	R Review and recla			CIA			
	ORMATION CUSTO						
11	R Backup recovery			ΙA			
12	R Basic input data						
16		and field comparison edits					
18		ansmission/ Transportation/ Stora		<u>C</u>			
19		ng of electronic authentication info	<u>ormation</u>	C			
20	R Environmental pr			IA O			
22		e media prior to reuse		C			
33 39	R Limit access to so	ecure areas		CI IA			
39 55		hod for re-writeable media		C			
<u> </u>	IV OSE MISPOSAL ITIEL	HOU TO LE-WITTE ADIE MEUIA					
SF V	NORKFORGE (INFO	DRMATION USER) CONTROLS					
15		dentity and access rights of reque	ester	С			
30		IFIDENTIALITY-HIGH"		C			
35		formation in e-mail subject line		Č			
41		rinting/faxing (immediate)		C			
49	R Secure area			CI			
50		nedia when unattended		CI			
51	R Situational aware	ness during verbal communication	าร	С			
53	R Transportation ha	andling controls for paper		С			
		TY OFFICER (ISO) CONTROLS					
11		removal process (audit)		С			
47	R Review security p	procedures and controls (annually	)	CIA			

CONFIL	DENTIALITY (C): HIGH	INTEGRITY (I): MODERATE	AVAILABILITY (A): HIGH
Glossary X-			
Ref #	R=Required O=Option	al	CIA
STA	TE ENTITY (SE) CONTRO	LS	•
2	R Access approval/remo	val process in place	С
7	R Address recovery in SI	Business Continuity/Disaster Recove	ery Plan A
9	R Approved electronic st	orage media and devices	С
10	R Approved storage facil	it <u>v</u>	CI
13	R Chain of custody for pl	nysical media	С
17	R Destroy when no long	<u>er n eed ed</u>	С
23	R Formal change contro	procedures for information systems	I
24	R Formal test plans and	documented results for information sys	stems I
29	R Information classificati	on and inventory	CIA
36 R Non-Disclosure Agre		ment (NDA), Acceptable Use Policy, M	<u>Memorandum of</u> C
	Understanding (MOU) or	similar device for third-parties	
38	R Privacy disclaimer on e	e-mail and fax cover sheets	C
40	R Reproduction authoriz		C
48	R Review system and ap	plication security logs	CI
56	R Written approval for Tr	ansmission, Transportation and Storag	ge (TTS) C
INEC	I DRMATION OWNER CONT	TROL 6	
5		nformation owner (written & cc: exec)	С
6	R Access provided to mo		A
44	R Review access lists (a		CI
45 45	R Review and reclassify		CIA
70	It Iteview and reclassify	<u>Imormation</u>	Oir
INFO	RMATION CUSTODIAN C		
8	R Alternate means of ava	<u>ailability</u>	A
11	R Backup recovery proce		IA
12	R Basic input data valida		I
16	R Data plausibility and fie		<u> </u>
18		ssion/ Transportation/Storage (TTS)	
19		electronic authentication information	С
20	R Environmental protecti		IA
21	R Environmental protecti		IA
22	R Erase re-writeable med		C
33	R Limit access to secure	<u>areas</u>	CI
37	R Off-site backup		A
39	R Regular backup		IA
52	R Test recovery of backu		IA
55	R Use disposal method f	or re-writeable media	C
SF I	<u> </u>   Workforce (Informat	ION USER) CONTROLS	
15		y and access rights of requester	ГС
30	O Label: "NYS CONFIDE		C
35		ation in e-mail subject line	C
41	R Retrieval when printing		C
49	R Secure area	graning (illimodiate)	CI
50	R Secure physical media	when unattended	CI
51		during verbal communications	C
53	R Transportation handlin		C
	Tanaportation nandil	is control of paper	
INFO	DRMATION SECURITY OF	FICER (ISO) CONTROLS	
1	R Access approval/remo		С
		dures and controls (annually)	CIA

CONF	IDENTIALITY (C): HIGH	INTEGRITY (I): HIGH	AVAILABILITY (A LOW	<b>)</b> :
Glossary X-Ref #	R=Required O=Optiona	-		CIA
	ATE ENTITY (SE) CONTRO			OIA
2	R Access approval/remov			С
9	R Approved electronic sto			C
10	R Approved storage facilit	-		CI
13	R Chain of custody for ph			C
17	R Destroy when no longe			C
23		procedures for information systems		Ī
24		documented results for information system	ns	i
29	R Information classification		110	CIA
36		ment (NDA), Acceptable Use Policy, Mem	norandum of Understanding	C
00	(MOU) or similar device fo		<u> </u>	Ū
38		e-mail and fax cover sheets		С
40	R Reproduction authorize			C
48	R Review system and app			CI
56		ansmission, Transportation and Storage (	TTS)	C
	TO WITHOUT APPROVATION THE	aremiseren, maneperation and eterage (	110,	
INF	ORMATION OWNER CON	NTROLS		
5		nformation owner (written & cc: exec)		С
44	R Review access lists (an			CI
45	R Review and reclassify in			CIA
INF	ORMATION CUSTODIAN	CONTROLS		
11	R Backup recovery proce			ΙA
12	R Basic input data validat			1
16	R Data plausibility and fiel			i
18		ssion/ Transportation/Storage (TTS) Out	tside the SE	C
19		electronic authentication information		C
20	R Environmental protection			IA
21	R Environmental protection			IA
22	R Erase re-writeable med			C
33	R Limit access to secure a			CI
34	R Message integrity	<u>areas</u>		<u> </u>
39	R Regular backup			IA
52	R Test recovery of backup	n data		IA
55	R Use disposal method for			C
JJ	iv ose disposal illetillogito	UTTE-WITTEADIE HIEUTA		
SF	WORKFORCE (INFORMA	ATION LISER) CONTROLS		
15		v and access rights of requester		С
30	O Label: "NYS CONFIDEN			C
35	R No confidential informa			C
41	R Retrieval when printing			C
49	R Secure area	greating (miniodiato)		CI
50	R Secure physical media	when unattended		CI
51		during verbal communications		C
53	R Transportation handling			C
	Transportation natural	g control of paper		
	<u> </u>			
INI	CORMATION SECURITY O	SEFICER (ISO) CONTROLS		
	R Access approval/remov		ı	
1 47	R Access approval/remov			C CIA

CONF	IDENTIALITY (C): HIGH	INTEGRITY (I): HIGH	AVAILABILITY (A MODERATE	<b>v)</b> :
Glossary X-Ref #	R=Required O=Optiona	al		CIA
	ATE ENTITY (SE) CONTRO	DLS		
2	R Access approval/remov	al process in place		С
9	R Approved electronic sto	rage media and devices		С
10	R Approved storage facili			CI
13	R Chain of custody for ph	<u>ysical media</u>		С
17	R Destroy when no longe			С
23	R Formal change control	procedures for information systems		l
24		ocumented results for information syst	tems	
29	R Information classification			CIA
36	R Non-Disclosure Agreem (MOU) or	nent (NDA), Acceptable Use Policy, M	emorandum of Understanding	С
38	R Privacy disclaimer on e	-mail and fax cover sheets		С
40	R Reproduction authorize	d by information owner		С
48	R Review system and app			CI
56	R Written approval for Tra	nsmission, Transportation and Storage	e (TTS)	С
	FORMATION OWNER CO			
5		nformation owner (written & cc: exec)		С
6	R Access provided to mo			Α
44	R Review access lists (an			CI
45	R Review and reclassify i	<u>nformation</u>		CIA
	FORMATION CUSTODIAN			
11 12	R Backup recovery proce R Basic input data validat			IA
<u>16</u> 18	R Data plausibility and fie	id comparison edits ssion/ Transportation/ Storage (TTS) (	Outside the SE	C
19		electronic authentication information	<u>Juiside life SE</u>	C
20	R Environmental protection			IA
21	R Environmental protection			IA
22	R Erase re-writeable med			C
33	R Limit access to secure			CI
34	R Message integrity	areas		I
39	R Regular backup			IA
52	R Test recovery of backup	n data		IA
55	R Use disposal method for			C
SF	WORKFORCE (INFORMA	TION USER) CONTROLS		
15		and access rights of requester		С
30	O Label: "NYS CONFIDEN			C
35	R No confidential informa			C
41	R Retrieval when printing			C
49	R Secure area			CI
	R Secure physical media	when unattended		CI
			C	
50 51	R Situational awareness (	dining verbai communications		
	R Transportation handling			С
51 53		controls for paper		С
51 53	R Transportation handling	controls for paper  OFFICER (ISO) CONTROLS		C

CONF	FIDENTIALITY (C): HIGH	INTEGRITY (I): HIGH	AVAILABILITY (A): HIGH
Glossary X-Ref #	R=Required O=Optiona	ıl	CIA
ST	TATE ENTITY (SE) CONTR	OLS	
2	R Access approval/remov	al process in place	С
7		Business Continuity/Disaster Recov	ery Plan A
9	R Approved electronic sto		С
10	R Approved storage facili		CI
13	R Chain of custody for ph		С
17	R Destroy when no longe		C
23		procedures for information systems	
24		ocumented results for information sy	stems I
29	R Information classification		CIA
36	R Non-Disclosure Agreen	nent (NDA), Acceptable Use Policy, N	
00	Understanding (MOU) or	ione (ND/I), Accoptable Goo Folloy, I	womorunaum or
38	R Privacy disclaimer on e	mail and fax cover sheets	С
<u>36</u> 40	R Reproduction authorize		C
40 48	R Review system and app		CI
<u>48</u> 56		nsmission, Transportation and Stora	
30	R Willen approvarior fra	insmission, fransportation and Stora	ge (115)
	FORMATION ON THE CO.	ALTROL O	
	FORMATION OWNER CO		
5		formation owner (written & cc: exec)	C
6	R Access provided to mo		A
44	R Review access lists (an		CI
45	R Review and reclassify i	nformation	CIA
	<u> </u>		
	FORMATION CUSTODIAN		
8	R Alternate means of available		A
11	R Backup recovery proce		IA
12	R Basic input data validat		<u> </u>
16	R Data plausibility and fie	d comparison edits	I
18		ssion/ Transportation/Storage (TTS)	Outside the SE C
19	R Encryption/hashing of e	electronic authentication information	С
20	R Environmental protection	on measures	IA
21	R Environmental protection	on measures monitoring	IA
22	R Erase re-writeable med		С
33	R Limit access to secure		CI
34	R Message integrity		
37	R Off-site backup		A
39	R Regular backup		IA
52	R Test recovery of backur	data	IA
55	R Use disposal method for		C
	200 0.00000000000000000000000000000		
SF	WORKFORCE (INFORM	ATION USER) CONTROLS	
15		and access rights of requester	С
30	O Label: "NYS CONFIDE		C
35	R No confidential informa		C
41	R Retrieval when printing		C
		riaxing (illillieurate)	
49	R Secure area	when weatteneded	Cl
EC	R Secure physical media	when unattended luring verbal communications	CI
<u>50</u>			C
51			_
	R Transportation handling		С
51 53	R Transportation handling	g controls for paper	С
51 53 IN	R Transportation handling FORMATION SECURITY	controls for paper  OFFICER (ISO) CONTROLS	
51 53	R Transportation handling FORMATION SECURITY ( R Access approval/remove	controls for paper  OFFICER (ISO) CONTROLS	C CIA

	CONFIDENTIALITY CONTROLS
Glossary X-Ref #	R=Required O=Optional
LO	W 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
МО	DERATE 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
HIG	SH 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
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)

NYS-S14-003 APPENDIX A

	INTEGRITY CONTROLS						
Glossary X-Ref # R=Required O=Optional							
LOW CONTROLS							
12 R Basic input data validation							
29 R Information classification and inventory							
43 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
LO	W CONTROLS
29	R Information classification and inventory
45	R Review and reclassify information
46	R Review security procedures and controls
MO	DERATE CONTROLS
6	R Access provided to more than one person
11	R Backup recovery procedures
20	R Environmental protection measures
39	R Regular backup
HIG	SH 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

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION/CLARIFICATION	CIA	CONTROL RATING	SUGGESTED ROLE
1	Access approval/removal process (audit)	R	Authorization	Audit the access approval/removal process at least annually.	С	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.	С	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.	С	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.	С	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 blanketapproval for a user or groups of users.	С	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.	Α	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.	С	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.	С	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.	С	MODERATE	User

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION/CLARIFICATION	CIA	CONTROL RATING	SUGGESTED ROLE
	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.	С	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).	С	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	С	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).	С	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

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION/CLARIFICATION	CIA	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	С	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.	l	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	Classify information assets on an ongoing basis. Information classification must be readily available to all users.     Maintain a written or electronic inventory of all information assets.	CIA	LOW	State Entity
30	Label: "NYS CONFIDENTIALITY- HIGH"	Ο	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.	С	HIGH	User
31	Label: "NYS CONFIDENTIALITY- LOW"	0	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.	С	LOW	User
32	Label: "NYS CONFIDENTIALITY- MODERATE"	0	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.	С	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.	С	HIGH	User

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION/CLARIFICATION	CIA	CONTROL RATING	SUGGESTED ROLE
	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.	С	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.	Α	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.	С	LOW	State Entity
39	Regularbackup	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.	С	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.	С	HIGH	User
42	Retrieval when printing/faxing (timely)	R	Reproduction	Pick up copies or printouts as soon as practical.	С	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

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION/CLARIFICATION	CIA	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.	С	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.	С	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.	С	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).	С	LOW	Custodian
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.	С	HIGH	State Entity