



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 Policy	No: NYS-P13-001
IT Policy Name: Information Security Exception Policy	Updated: 09/19/2014
	Issued By: NYS ITS State Chief Information Officer Policy Owner: Enterprise Information Security Office

1.0 Purpose and Benefits of the Policy

This purpose of this policy is to provide a method for obtaining an exception to compliance with a published NYS Office of Information Technology (ITS) information security policy or standard.

2.0 Enterprise IT Policy Statement

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the NYS Office 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 of the Policy

This policy applies to all "State government entities," as defined in NYS Executive Order 117.

This policy only applies to ITS information security policies and standards owned by the Enterprise Information Security Office (EISO).

4.0 Policy Statement

An exception may be granted by the Chief Information Security Officer (CISO) of ITS, or their designee, for non-compliance with a policy or standard resulting from:

- Implementation of a solution with equivalent protection.
- Implementation of a solution with superior protection.
- Impending retirement of a system.
- Inability to implement the policy or standard due to some limitation (i.e., technical constraint, business limitation or statutory requirement).

Exceptions are reviewed on a case-by-case basis and their approval is not automatic. Exceptions that are granted will be for a specific period of time, not to exceed one year. Requesters may apply for an extension of the exception if it is still required.

The exception request must be submitted on a completed Exception Request Form (Appendix A) and must include:

- Description of the non-compliance
- Anticipated length of non-compliance
- Proposed assessment of risk associated with non-compliance
- Proposed compensating controls for managing the risk associated with non-compliance
- Proposed corrective action plan
- Proposed review date, if less than one year, to evaluate progress toward compliance
- The Exception Request Form must be signed by the following:
 - Information/business owner
 - Chief Information Officer
 - Information Security Officer/designated security representative
 - Commissioner/Executive Deputy Commissioner

If the non-compliance with the security policy or standard is due to a superior solution, an exception is still required and will normally be granted until the published policy or standard can be revised to include the new solution.

Upon submission of the Exception Request Form, the EISO will contact the requester to confirm receipt and request additional information, if needed. Once all required information has been received, the EISO will either grant or deny the request.

Upon approval, the EISO will send the approved Exception Request Form to the requestor. If the request is denied, the Exception Request Form will be returned with a brief explanation of why the EISO denied the request.

In the event that the request is denied, the Commissioner/Executive Deputy Commissioner and the CIO who signed the Exception Request Form may request a meeting with the State Chief Information Officer and the CISO to discuss the circumstances giving rise to the request and means of addressing those circumstances.

5.0 Policy Compliance

This policy shall take effect upon publication. The Policy Unit shall review the policy at least once every year to ensure relevancy. The Office may also assess agency compliance with this policy. 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.

The Exception Request Form ([Appendix A](#)) must be submitted to the Enterprise Information Security Office at eiso@its.ny.gov or State Office Campus – Building 7A, 1220 Washington Avenue, Albany, New York 12242.

6.0 Definitions of Key Terms

Not Applicable

7.0 ITS Contact Information

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

Policy Owner
Attention: Enterprise Information Security Office
New York State Office of Information Technology Services
1220 Washington Avenue – Bldg. 7A, 4th Floor
Albany, NY 12242
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
10/18/2013	Original Policy Release	Thomas Smith, Chief Information Security Officer
09/19/2014	Policy Review – no changes	Deborah A. Snyder, Acting Chief Information Security Officer
09/19/2015	Scheduled Policy Review	

9.0 Related Documents



ENTERPRISE INFORMATION SECURITY OFFICE
EXCEPTION REQUEST FORM

Section 1: Exception Information

1.1 Requestor Information

Name:	Phone:	Date:
<input type="text"/>	<input type="text"/>	<input type="text"/>
Business Unit:	E-mail:	
<input type="text"/>	<input type="text"/>	

1.2 Exception Details

Policy Reference:	Standard Reference(s):	Exception End Date (no more than one year):
<input type="text"/>	<input type="text"/>	<input type="text"/>

Agency(s) Impacted:

System(s)/Hardware Impacted <i>(if applicable)</i>	Will this impact the processing, storage and/or transmission of PPSI?
<input type="text"/>	<input type="text"/>

1.3 Reason for Exception Request

1.4 Description/Assessment of Risk

1.5 Compensating Controls *(to mitigate risk associated with noncompliance)*

1.6 Corrective Action Plan

Confidential when Completed

Confidential when Completed

Section 2: Requestor Authorizations

2.1 Information/Business Owner	Name: <input type="text"/>
2.2 Information Security Officer (ISO) / Designated Security Representative	Name: <input type="text"/>
2.3 Chief Information Officer (CIO)	Name: <input type="text"/>
2.4 Commissioner/Executive Deputy (or equivalent)	Name: <input type="text"/>

Submit via Email

OR

Please print and return to:

Print Form

eiso@its.ny.gov or
State Campus, Building 7A, 1220 Washington Avenue, Albany, NY 12242

Section 3: Exception Approval/Denial

Exception: <input type="text"/>	Proposed Review Date: <input type="text"/>
--	---

Reason for Denial:

Only enter if Exception is Denied

3.1 Enterprise Chief Information Security Officer/Deputy CISO	Name: <input type="text"/>
--	----------------------------