NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

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

New York State Information Technology Policy	**No:** NYS-P13-001
IT Policy: **Information Security Exception Policy**	**Updated:** 03/10/2017
	Issued By: NYS Office of Information Technology Services **Owner:** Enterprise Information Security Office

1.0 Purpose and Benefits

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 Authority

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

3.0 Scope

This policy is promulgated pursuant to New York State Information Technology Policy NYS-P03-002, Information Security, and applies to ITS, all State Entities (SE) that receive services from ITS, and affiliates of same (e.g., contractors, vendors, solution providers), which have access to or manage SE information. It also serves as recommended practice for the State University of New York, the City University of New York, non-Executive branch agencies, authorities, NYS local governments and third parties acting on behalf of same. This policy only applies to ITS information security policies and standards owned by the Enterprise Information Security Office (EISO).

4.0 Information 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 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 Compliance

This policy 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 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 http://www.its.ny.gov/glossary.

7.0 Contact Information

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

Enterprise Information Security Office
Reference: NYS-P13-001
NYS Office of Information Technology Services
1220 Washignton Avenue, Bldg 5
Albany, NY 12242
Telephone: (518) 242-5200
Email: EISO@its.ny.gov

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

8.0 Revision History

This policy shall be reviewed at least once every year to ensure relevancy.

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
03/10/2017	Update to Scope, contact information and rebranding	Deborah Snyder, Deputy Chief Information Security Officer

9.0 Related Documents

Identity Assurance Policy

Identity Assurance Standard

Authentication Tokens Standard

Security Logging Standard

NIST Special Publication 800-63, Electronic Authentication Guideline

NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

Enterprise Information Security Office - Exception Request Form

Confidential when completed

Section 1: Exception		
1.1 Requestor Information		
Name:	Phone:	Date:
Business Unit:		
Email:		
1.2 Exception Details		
Policy Reference:	Standard Reference:	Exception End Date: (no more than one year)
Agency(s) Impacted:		
System(s) Hardware Impacted (if applicable):		
Will this impact the process, stage and/or transmission of PPSI? **Yes** _____ **No** _____		
1.3 Reason for Exception Request		
1.4 Description/Assessment Risk		
1.5 Compensating Controls (to mitigate risk associated with non-compliance)		
1.6 Corrective Action Plan		

Section 2: Requestor Authorizations		
2.1 Information/Business Owner:	X_____ Information/Business Owner	**Date:**
2.2 Information Security Officer (ISO)/Designated Security Representative:	X_____ ISO	**Date:**
2.3 Chief Information Officer (CIO):	X_____ Agency/Cluster CIO	**Date:**
2.4 Commissioner/Executive Deputy (or equivalent):	X_____ Commissioner/Executive Deputy	**Date:**
Return to: eiso@its.ny.gov	NYS Office of Information Technology Services Enterprise Information Security Office 1220 Washington Avenue, Bldg. 5 Albany, NY 12242 Phone (518) 242-5200	

Section 3: Exception Approval/Denial ***(For EISO Use Only)***	
Exception: ____ **Approved** ____ **Denied**	**Proposed Review Date:**
Reason for Denial:	

3.1 Enterprise Chief Information Security Officer/Deputy CISO:		**Date:**