New York State Information Technology Policy	**No:** NYS-P13-001
IT Policy: **Information Security Exception Policy**	**Updated:** 10/11/2022
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

The purpose of this policy is to provide a method for obtaining an exception to compliance with a published security policy or standard issued by New York State (NYS) Office of Information Technology Services (ITS).

2.0 Authority

Section 103(10) of the State Technology Law provides ITS with the authority to establish statewide technology policies, including technology and security standards. Section 2 of Executive *Order No. 117[1]*, 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 policy applies to all "State Entities" (SE), 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

---

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021

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 policy, it must include the requirements set forth in this one.

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. Justification for approval of policy or standard exceptions include, but are not limited to:

- Implementation of a solution with equivalent protection to the requirements in the CISO policy or standard.

- Implementation of a solution with superior protection to the requirements in the CISO policy or standard.

- Impending retirement of a system.

- Inability to implement the policy or standard due to some limitation (e.g., 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. Upon expiration of the exception, an extension of the exception may be requested, 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 or mitigation plan

- Proposed review date to evaluate progress toward compliance

- The Exception Request Form must be signed by the following:

  o Information/Business Owner

  o Information Security Officer (ISO)/Designated Security Representative

o Chief Information Officer (CIO): (Agency/Portfolio CIO)

Commissioner/Executive Deputy Commissioner (or equivalent) If the non-compliance with the security policy or standard is due to a superior solution, an exception is still required. Such instances will be evaluated for possible inclusion into published policy or standard.

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

Upon approval, the CISO's office 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 CISO 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 CIO 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 required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

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:

Chief Information Security Office
Reference: NYS-P13-001
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@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 should be reviewed consistent with the requirements set forth in *NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

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
02/10/2017	Update to Scope, contact information and rebranding	Deborah Snyder, Deputy Chief Information Security Officer
02/07/2020	Updated Authority, Scope, and Contact Information	Karen Sorady, Acting Chief Information Security Officer
05/20/2021	Updated Scope language	Karen Sorady,Acting Chief Information Security Officer
10/11/2022	Scheduled review and update, removal of one year limitation, grammatical changes, and other minor revisions.	Chris DeSain, Chief Information Security Officer

9.0 Related Documents

NYS-P13-001 Information Security Exception Policy Form