NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Odysseus Marcopolus, Chief Operating Officer
P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212
www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 111 – Information Security Managing Exceptions Policy	**POLICY NO:** 08-02-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 06/02/2008
	VERSION: 2.0	**LAST REVIEWED:** 11/15/2011

1 PURPOSE

In order to successfully protect information assets and manage risks associated with the use of those assets, an information security program has been established (See Circular 08-01-NJOIT). The foundation of managing risks and providing due care to information assets relies on the implementation of and compliance with uniform information security policies, standards, and procedures. There are however circumstances when compliance may not be feasible. Because non-compliance represents risks to the enterprise, the Chief Technology Officer (CTO), must be made aware of and underwrite all non-compliance exceptions.

2 AUTHORITY

This policy is established under the authority of 08-01-NJOIT, *100 - Information Security Program*.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular to comply with changes in NJOIT or other agency policies.

3 SCOPE/APPLICABILITY

This policy applies to all personnel including employees, temporary workers, volunteers, contractors and those employed by contracted entities, and others who administer enterprise information resources, within the Executive Branch of State government.

4 POLICY

This document specifies policies, standards, and procedures (PSP) for requesting, documenting, approving, and managing exceptions[1] to information security policies, standards, and/or procedures. The following policy prescribes how exceptions shall be managed:

4.1.1 All requests for compliance exceptions must be based on a valid constraint that prevents full compliance with the policy, standard, or procedure.

4.1.2 Requests for compliance exception approval for any information security policy, standard, or procedure must be made to the Statewide Information Security Officer (SISO) or originated by the SISO in writing. The requestor shall include in the request proposed alternative mechanisms (procedures, technology, or physical controls) to compensate for any risks associated with the exception.

4.1.3 The SISO, with assistance from appropriate knowledge experts where required, shall review the exception and proposed alternative mechanisms and provide recommendations to the Chief Technology Officer (CTO).

4.1.4 Final approval for an exception, if granted, shall be provided in writing by the CTO and maintained by the SISO.

4.1.5 The SISO will fully document the exception and alert all appropriate parties of the vulnerability.

4.1.6 The selection of an alternative security mechanism to compensate for an exception shall be considered temporary. The SISO shall track and review exceptions for as long as they exist to determine:

4.1.6.1 If the exception is still needed.

4.1.6.2 If technology, budget, personnel, or other resources are available to correct the exception.

4.1.6.3 If new projects or initiatives can or will remediate the exception.

[1] Within this policy, the term "exception" includes all degrees (partial, full, etc.) of non-compliance.

5 PROCEDURES

5.1.1 The requestor of an exception to a PSP shall document, at a minimum, the following information in the Exception Request Form:

5.1.1.1 General description of exception.

5.1.1.2 Proposed alternative measures to be implemented.

5.1.1.3 Proposed exception duration.

5.1.1.4 Criticality and/or Sensitivity of Data or Hardware involved in exception.

5.1.2 The SISO, upon receiving or originating the request for deviation or exception, shall:

5.1.2.1 Review and determine:

5.1.2.1.1 The validity of the request as it relates to the overall Statewide Office of Information Security goals and objectives and any risk mitigation considerations or compliance mandates that impact the request.

5.1.2.1.2 Whether additionally the exception violates any dominant policies (e.g., Federal, State).

5.1.2.1.3 Whether the proposed alternative measures provide the appropriate compensating controls.

5.1.2.1.4 Whether other alternative approaches for handling the requested exception may exist.

5.1.2.1.5 Whether the proposed plan and timeframe for corrective actions are reasonable given the risk.

5.1.2.2 The SISO shall solicit input from key management and units that may be affected by the exception.

5.1.2.3 Present the recommendation to the CTO for a final decision.

5.1.2.4 Coordinate with the Agency/Unit Director to ensure that the appropriate alternative control methods agreed upon in granting the exception has been implemented and that the request is still valid.

5.1.2.5 The SISO shall maintain copies of all exceptions.

5.1.2.6 On an on-going basis (no less that annually), the SISO shall review approved exceptions with the Agency/ Unit Director to determine if the exception is still valid.

5.1.3 Should the CTO approve the exception, copies of the approved exceptions shall be maintained by the SISO who will track it for references.

Additional copies will be provided to the originator or the originating Agency Director.

6 RESPONSIBILITIES

6.1.1 Chief Technology Officer (CTO)

The CTO shall be apprised of and must approve all exceptions.

6.1.2 EEO/AA/Ethics

EEO/AA/Ethics resources shall perform legal reviews and provide opinions as necessary.

6.1.3 Agency/ Unit Directors

Agency/ Unit Directors are responsible for identifying PSP non-compliance within their areas of responsibility, attempting to remediate the non-compliance and if that is not possible, requesting and internally tracking exception requests.

6.1.4 Statewide Information Security Officer

The Statewide Information Security Officer is responsible for managing exceptions as denoted in this policy.