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 205 – Certification and Accreditation Policy	**POLICY NO:** 14-13-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 04/10/2014
	VERSION: 1.0	**LAST REVIEWED:** 04/10/2014

1 PURPOSE

The purpose of this policy is to ensure validation of compliance with security requirements for systems, applications, system software, and other technologies before they are deployed into a production environment. This policy also requires appropriate reviews and testing of configurations, functionality, and prevention and protection controls. It also is designed to ensure compliance with specifications, regulations, standards and objectives identified during each phase of the System Development Life Cycle (SDLC).

2 AUTHORITY

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. This policy defines the role of the New Jersey Office of Information Technology (NJOIT) with regard to technology within the Executive Branch community of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.

3 SCOPE

This policy applies to all New Jersey systems that process, transmit, or store State information. This policy also applies to all State personnel including employees, temporary workers, volunteers, contractors and those employed by contracted entities, as well as any others who administer State information resources.

4 POLICY

Certification and Accreditation (CA2) establishes a review process and guidance for protecting and safeguarding a State system or application; hereafter referred to as an "asset". The CA2 process consists of five phases: Initiation, Certification, Accreditation, Continuous Monitoring, and Reaccreditation.

4.1.1 Initiation

During the Initiation Phase, the business owner and IT staff review and define the business and technology requirements, security needs, and classification of the applicable assets.

4.1.2 Certification

The Certification phase consists of assessments for security, vulnerability and risk.

4.1.3 Accreditation

The Accreditation phase is designed to evaluate production readiness and security compliance.

4.1.4 Continuous Monitoring and Maintenance

The Continuous Monitoring and Maintenance phase requires ongoing monitoring of State assets for security threats.

4.1.5 Reaccreditation Process

The Reaccreditation Process requires each agency to sustain their asset accreditation requirements.

The Statewide Information Security Officer (SISO) and the Statewide Office of Information Security are responsible for directing the Certification and Accreditation of State assets.

5 RESPONSIBILITIES

5.1.1 Statewide Office of Information Security (SOIS)

The SOIS is responsible for overseeing the certification and accreditation of the Statewide Systems and Networks while performing the following duties:

5.1.1.1 Administering the certification and accreditation process and periodically evaluating whether the program is being implemented effectively.

5.1.1.2 Developing and implementing Security Policies, Standards and Procedures.

5.1.1.3 Reviewing requested exceptions to Security Policies, Standards and Procedures.

5.1.1.4 Providing guidance and expertise in IT security remediation of security vulnerabilities.

5.1.1.5 Maintaining awareness of security status of the Statewide Systems and Network infrastructure.

5.1.2 Agencies

Each Agency has the ultimate responsibility for the protection of its information from disclosure, loss, or misuse. As such, each agency must maintain a thorough knowledge base and develop documentation of the security controls protecting these assets. It must also be prepared for assessments of these security controls.

6 EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date.

A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. Exceptions and non-compliance with this policy shall be managed in accordance with OIT Policy 08-02-NJOIT, *111 – Information Security Managing Exceptions.*