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 121- Confidential and/or Personally Identifiable Information Policy	**POLICY NO:** 14-33-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 10/24/2014
	VERSION: 1.0	**LAST REVIEWED:** 10/24/2014

ATTN: Directors of Administration and Agency IT Leaders

1 PURPOSE

The purpose of this policy is to ensure state agencies develop a secure and consistent approach to accessing and handling Confidential and Personally Identifiable Information (PII). This policy provides the requirements for protecting the privacy of people who have PII that resides on State databases or in electronic and paper files and/or any other type of media. It also covers contracted entities who gain access to State of New Jersey physical facilities, data or computer systems. This policy lays out the basic handling expectations for all types of PII.

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 New Jersey Office of Information Technology's (NJOIT) role 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 pertains to anyone handling any PII that is collected, processed or maintained on any infrastructure and systems operated by the State of New Jersey and/or its contracted entities. Additionally, this policy seeks to appropriately set the privacy expectations of those interacting with State government.

By accessing the State's network or software applications, a user agrees to adhere to the State's policies, including agency specific policies, regarding their use.

4 DEFINITION

Please refer to the statewide policy glossary at http://www.state.nj.us/it/ps/glossary/index.html

5 POLICY

It is the policy of the State of New Jersey to protect the PII of employees, clients and citizens.

This policy uses PII in the general sense to identify as many potential sources of PII as possible. (e.g. databases, shared networks drive, backup tapes, hosted sites).

NIST Special Publication 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" defines PII as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

5.1.1 Departments and agencies should locate and identify all PII residing in their environments and infrastructure and also any State data that may contain PII that is managed by third party hosted external entities.

5.1.2 Departments and agencies shall minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.

5.1.3 Department and agencies should ensure that retired hardware no longer contains PII and that proper sanitization techniques are applied. The proper sanitization techniques will be addressed in accordance with 09-10-NJOIT, *152 – Information Disposal and Media Sanitization Policy*.

5.1.4 Department and agencies should categorize their PII by the PII confidentiality impact level (e.g. Confidential, Restricted, or Public).

5.1.5 Department and agencies should apply the appropriate safeguards, including encryption, for PII based on the asset classification level. This should be accomplished with the understanding that some data is more sensitive than other information, and should be protected in a more secure manner. (e.g. Secure, Confidential, or Personal). For data that is comingled, the highest classification level shall apply. The asset classification controls will be addressed in accordance with 08-04-NJOIT, *130 – Information Asset Classification Control Policy*.

5.1.6 Department and agencies should follow 11-02-NJOIT, *190 – Information Security Incident Management Policy* for handling a breach involving PII.

6 RESPONSIBILITIES

6.1 Employee

Employees shall follow this policy and all agency confidential and sensitive information policies and procedures. Users should report any misuse or policy violations to their supervisor or agency IT director.

6.2 Agency

Agencies are responsible for developing agency guidelines, procedures, and internal controls for monitoring compliances that are in accordance with this policy.

Agencies shall furnish their current employees copies of this notice, and shall furnish all new employees copies of this policy concurrent with authorizing them to use agency computers.

Agencies shall discipline their employees for violations of this policy or any standards or guidelines referenced.

Agencies shall promote the awareness of acceptable collection, storage and dissemination of PII by training employees.

Agencies will authorize the collection and maintenance of the minimum information needed to achieve its statutorily defined purposes. Further, the agency is solely authorized to disclose maintained data, whether that release serves its statutorily defined purposes or under the provisions of the New Jersey's Open Public Records Act (OPRA).

6.3 Chief Information Security Officer

The Chief Information Security Officer is responsible for setting the applicable privacy policies for the implementation and use of information and telecommunications technologies.

7 EXCEPTIONS AND NONCOMPLIANCE

Failure to comply with this policy may result in disciplinary action. A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. All requests for a compliance exception shall be made to the Chief Information Security Officer (SISO) in writing.