



STATE OF NEW JERSEY IT CIRCULAR Title: 201- State of New Jersey On-line Privacy Policy	NO: 13-09-NJOIT		SUPERSEDES: 06-05-NJOIT	
	LAST REVIEWED: December 19, 2013		DATE PUBLISHED: December 19, 2013	
	VERSION: 1.1	EFFECTIVE DATE: Date of Signature		
	FOR INFORMATION CONTACT: Office of Policy and Planning			

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

To ensure that the State has the best possible controls and procedures for the protection of the private information of any person who interacts with New Jersey Executive Branch Agencies.

II. 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 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.

III. SCOPE

This policy applies to all public websites of State agencies in the Executive Branch.

IV. DEFINITIONS

Please refer to the Statewide Policy Glossary at <http://www.nj.gov/it/ps/glossary/>.

V. POLICY

A. All New Jersey Executive Branch Agencies that operate Internet Web or on-line services shall have privacy statements that are prominently displayed on their home pages and any other public entry page where personally identifiable information is collected or transmitted. Personally identifiable information means information that can be used to identify an individual, including a Social Security number, name, address other than the five digit ZIP code, driver identification

number, telephone number and e-mail address. The statements shall be developed in accordance with the Principles of Fair Information Practices as recommended by the Federal Trade Commission and in consultation with agency legal counsel. The privacy statement shall be easy to find, read and understand. The statement should inform website users when personally identifiable information is collected and describe how it will be used. The statement should also advise users if there will be any third-party distribution of the information and of the choices available regarding collection, use, and distribution of the information.

- B.** Following promulgation of this policy, each State agency that maintains a website requiring the collection or transmission of personally identifiable information will conduct a transaction risk assessment. Based on its assessment, each agency also will implement appropriate security and privacy safeguards. At a minimum, state websites that require or permit a citizen to enter the following information will encrypt the data using a SSL (Secure Sockets Layer) session or equivalent technology for managing the security of a message layer:
 - 1. Social Security Number or tax identification number
 - 2. Transaction payment information, i.e. credit card number
 - 3. Individual Name, address and other personal information
 - 4. Individual identification codes and passwords
 - 5. Individual medical and health information
 - 6. Individual financial information, i.e. income
- C.** State websites that permit the download of forms for completion and subsequent return via unencrypted e-mail should notify users of the risk in sending sensitive or personal information via e-mail over the Internet.
- D.** State agencies that elect to obtain information through the use of cookies shall notify the user when a cookie is being placed on a computer, describe the information to be collected via the cookie, and detail how the collected information will be used.
- E.** Agencies shall establish security procedures and practices for the storing, handling and disposing of electronic records that contain personally identifiable information so that unauthorized persons cannot intercept or change it.
- F.** Personally identifiable information will not be sold or distributed to non-governmental third parties for solicitation purposes unless permitted by law. The collection of personal data should be limited to that which is needed for legitimate public purposes, and data should be retained only as long as necessary.

Personally identifiable information should only be used for the purposes disclosed in the privacy policy statement.

- G.** Agencies that enter into contracts or agreements for sharing personally identifiable information with other entities must have contractual requirements that protect the information from inappropriate uses.
- H.** If an agency intends for its website to collect personally identifiable information, then the agency will notify the public that State and Federal laws, including statutes, rules, regulations and the common law, control the use of information held by the State. Citizens should be told how they can review their personal information and recommend corrections if it is inaccurate or incomplete.
- I.** Agency privacy statements shall include the name and contact information of a person who can address questions regarding the privacy statement and privacy practices of the Agency.
- J.** Agencies that provide Web pages directed at children shall comply with the Children's On-line Privacy Protection Act of 1998 (COPPA) and any other applicable State or Federal law. The Federal Trade Commission rule applies to websites or on-line services directed at children and to websites or on-line services where there is actual knowledge that the person from whom they seek information is a child. The requirements include but are not limited to:
 - 1.** Posting prominent links on their websites to a notice of how they collect, use, and/or disclose personal information from children.
 - 2.** With certain exceptions, notifying parents that the Agency wishes to collect information from their children and will obtain parental consent before collecting, using, and/or disclosing such information.
 - 3.** Not conditioning a child's participation in on-line activities on the provision of providing more personal information than is reasonably necessary to participate in the activity.
 - 4.** Allowing parents the opportunity to review and/or have their children's information deleted from the operator's database and to prohibit further collection from the child.
 - 5.** Establishing procedures to protect the confidentiality, security, and integrity of personal information they collect from children.

VI. ROLES AND RESPONSIBILITIES

A. Employee

1. To adhere to Statewide and agency security and confidentiality rules and procedures.
2. Maintain the confidentiality of individuals' personally identifiable information consistent with law.

B. Agency Senior Management

1. Designate a person or persons to act as the point of contact for all questions relating to access to information and privacy.
2. Ensure that employees who have access to the Internet are educated on the importance of maintaining the confidentiality of personal information.
3. Ensure that Web development efforts include consideration of privacy related issues.
4. Approve appropriate privacy statements, where required.

C. Agency Information Technology Unit and the new Jersey Office of Information Technology

1. Ensure that appropriate security safeguards are in place relating to the electronic transmission, electronic storage and electronic access of personal information.

VII. COMPLIANCE

Agencies, subject to this policy, 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 any portion of this policy. Exceptions and noncompliance shall be managed in accordance with Policy [08-02-NJOIT](#) 111 – Managing Exceptions.

Signature on File

E. STEVEN EMANUEL

**Chief Technology Officer-NJ Office of Information Technology
State Chief Information Officer**

12/19/2013

DATE