STATE OF ALABAMA

Information Technology Standard

STANDARD 681S2-00: PROTECTING PERSONALLY IDENTIFIABLE INFORMATION

Personally Identifiable Information (PII) is any information, not including a person's name, which used either alone or in conjunction with other information specifically identifies a person or a person's property. PII includes, but is not limited to, any of the following information related to a person:

- Date of birth
- Social Security number
- Driver's license number
- Financial services account numbers (including checking and savings accounts and credit or debit card numbers) or any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services

This standard establishes requirements for the protection of electronic records containing PII.

OBJECTIVE:

Protect PII electronic records from unauthorized modification, disclosure, or loss.

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) in Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), State of Alabama information system and data owners shall identify PII, evaluate the risk and impact of loss or unauthorized disclosure of PII, and implement PII confidentiality safeguards.

IDENTIFY PII

Identify all PII residing within the organization, under the control of the organization, or owned by the organization but residing on a third-party system (such as a system being developed and tested by a contractor).

Organizations may use a variety of methods to identify PII. Privacy threshold analyses (PTAs), also referred to as initial privacy assessments, are often used to identify PII. Conduct a PTA before the development or acquisition of a new information system or when a substantial change is made to an existing system. PTAs are used to determine if a system contains PII and whether a Privacy Impact Assessment (PIA) is required.

EVALUATE PII FOR RISK AND IMPACT

Evaluate PII for risk and impact of loss or unauthorized modification or disclosure and protected accordingly. Evaluate compilations of PII and identify those needing more stringent protection (such as for remote access or mobile computing).

A Privacy Impact Assessment (PIA) is a structured review of how information is handled to:

- Ensure handling conforms to applicable legal, regulatory, and policy requirements.
- Determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system.
- Identify and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

PII CONFIDENTIALITY SAFEGUARDS

Minimize the Use, Collection, and Retention of PII:

- PII collections should only be made where such collections are essential to meet the authorized business purpose and mission of the organization.
- Regularly review holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization‘s business purpose and mission.
- If the PII serves no current business purpose, then the PII should no longer be used or collected.

Security Controls:

All PII not explicitly cleared for public release shall be protected in accordance with information protection category Sensitive, as established in State IT Standard 681S1: Information Protection, with additional protections as required by this standard and organizational procedures. Specific security controls include:

- Control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists and role-based access controls).
- Enforce separation of duties for duties involving access to PII. For example, the users of de-identified PII data would not also be in roles that permit them to access the information needed to re-identify the records.
- Enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
- Prohibit or strictly limit remote access to PII. If remote access is permitted, ensure that the communications are encrypted.
- Prohibit or strictly limit access to PII from portable and mobile devices, such as laptops and smart phones.
- Monitor for events that affect the confidentiality of PII, such as unauthorized access.
- Regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
- Uniquely identify and authenticate users before granting access to PII.

- Restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm). This could also include portable and mobile devices with a storage capability.
- Label information system media and output containing PII to indicate how it should be distributed and handled. Examples of labeling are cover sheets on printouts and paper labels on digital media.
- Securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
- Protect digital and non-digital media and mobile devices containing PII that is transported outside the organization‘s controlled areas. Examples of protective safeguards are encrypting stored information and locking the media in a container.
- Sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
- Protect the confidentiality of transmitted PII. This is most often accomplished by encrypting the communications channel or by encrypting the information before it is transmitted.
- Protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape. This is usually accomplished by encrypting the stored information.
- When possible, employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events. An example is the use of data loss prevention technologies.

INCIDENT RESPONSE FOR BREACHES INVOLVING PII

Organizations shall prepare for potential data breaches and/or loss of PII by:

- Establishing clear roles and responsibilities to ensure effective management when an incident occurs.
- Establishing reporting procedures to ensure that compromise, loss, or suspected loss of PII is reported in accordance with incident response and data breach notification requirements.
- Planning in advance how, when, and to whom notifications should be made.
- Determining how incidents involving PII will be tracked within the organization.
- Determining what circumstances require the organization to provide remedial assistance (such as credit monitoring services) to affected individuals.

SUPPORTING DOCUMENTS:

- Information Technology Policy 681: Information Protection
- Information Technology Standard 681S1: Information Protection
- Information Technology Standard 681S3: Media Sanitization
- Information Technology Procedure 604P1: Cyber Security Incident Reporting

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
680-01S2	2/6/2007	Original document
681S2-00	09/01/2011	New number and format; content substantially revised