
	<b>PII Processing and Transparency Policy</b>		
<b>PR-DS-P2</b>			
<b>Effective Date:</b> 01/31/2025	<b>Date Approved:</b> 01/15/2025	<b>Version:</b> 1	<b>Page #:</b> 1 of 5

## GOVERNANCE

This document is governed by the IT Governance Policy which provides the following guidance:

- a. Roles and Responsibilities
- b. Policy Control Application
- c. Policy Compliance Requirements
- d. Policy Exemptions or Exceptions
- e. Policy Reviews and Updates

## SCOPE

This policy covers all State information and information systems, including those used, managed, or operated by a contractor, the State, or other organizations on behalf of the State. This policy applies to all employees, contractors, and users of information systems supporting the operation and assets of the State.

All information assets that process, store, receive, transmit, or otherwise impact the confidentiality, integrity, and accessibility of State data shall meet the security controls defined in this document as required by the State of Alabama's IT Governance Policy.

## PT-1 – POLICY AND PROCEDURES

This document addresses the requirements set forth by the State to implement the family of Personally Identifiable Information (PII) Processing and Transparency security controls at the organization, process and/or system level for all information assets and State data.



All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the required security controls in this policy based on the National Institute of Standards and Technology (NIST) SP 800-53r5 Security and Privacy Controls.

The "PT" designator identified in each section represents the NIST-specified identifier for the PII Processing and Transparency control family. The following subsections in this document outline the PII Processing and Transparency requirements that each agency must implement and maintain to be compliant with this policy. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The PII Processing and Transparency policy and procedures are essential for addressing controls within systems and organizations, requiring a robust risk management strategy. Collaboration between security and privacy programs is crucial to ensure comprehensive and effective policies tailored to the specific needs and risk of the State and executive-branch agencies.

As such, the State shall:

- a. Develop, document, and disseminate a PII Processing and Transparency Policy to all employees, contractors, and third-party service providers to address the following items:
  - i. The purpose and scope for the policy;
  - ii. The roles and responsibilities associated;

	<b>PII Processing and Transparency Policy</b>		
<b>PR-DS-P2</b>			
<b>Effective Date:</b> 01/31/2025	<b>Date Approved:</b> 01/15/2025	<b>Version:</b> 1	<b>Page #:</b> 2 of 5

- iii. The management commitment of the Secretary of OIT;
  - iv. The coordination required among organizational entities; and
  - v. The compliance items to be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
- b. Align State procedures to facilitate the implementation of the PII Processing and Transparency Policy and the associated information processing and transparency controls. Agencies requiring procedures not covered by the State policy may create their own documentation associated with the overall State policy; and
- c. Designate a Privacy Officer to manage the development, documentation, and dissemination of this policy and procedures and to ensure the policy is reviewed/updated at least every three (3) years or more frequently when State-defined events require.

## **PT-2 AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION**

The processing of PII is an operation or set of operations that the information system or organization performs with respect to PII across the information life cycle. Processing includes, but is not limited to, the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.

Many of the State’s agencies are subject to laws, executive orders, directives, regulations, or other policies which establish the organization’s authority to, and limitations on, certain types of processing of PII or establish other requirements related to the processing. As such, agency staff shall consult with the senior agency official for privacy and legal counsel regarding such authority, particularly if the organization is subject to multiple jurisdictions or sources of authority.

For those agencies where processing limitations are not determined according to legal authorities, the State PII Processing and Transparency Policy will govern how they process PII. While processing of PII may be legally permissible, privacy risks may still arise. Privacy risk assessments can identify the privacy risks associated with the authorized processing of PII and support solutions to manage such risks.

The State will consider applicable requirements to document in State policies to determine at what level the authority to process PII resides. For agencies under federal guidance, the authority to process PII is documented in privacy policies and notices, system of records notices, privacy impact assessments (PIAs), Privacy Act statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and other documentation.



Additionally, the State will take steps to ensure that PII is only processed for authorized purposes, including training personnel on the authorized processing of PII, as well as the monitoring and auditing the use of PII.

## **PT-3 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES**

Identifying and documenting the purpose for processing PII is crucial for the State and executive-branch agencies to understand and communicate the reasons behind PII processing.

Clear documentation enables system owners, operators, and individuals to make informed decisions and manage their privacy interests effectively. These purposes shall be described in privacy notices, policies, and compliance documents, including PIAs and System of Record notices.

PII shall be processed only for its intended purposes by trained personnel, who will monitor and audit

	<b>PII Processing and Transparency Policy</b>		
<b>PR-DS-P2</b>			
<b>Effective Date:</b> 01/31/2025	<b>Date Approved:</b> 01/15/2025	<b>Version:</b> 1	<b>Page #:</b> 3 of 5

processing activities. They shall also monitor changes in PII processing, consult with privacy officials and legal counsel, and implement mechanisms such as obtaining consent and revising policies to manage any new purposes and mitigate associated privacy risks.

The following shall be documented:

- a. Identify the purpose(s) and authority for processing PII within the State and executive-branch agencies;
- b. Description of the purpose(s) in privacy notices and policies of the organization;
- c. Restrictions on processing of PII to only that which is compatible with the identified purpose(s); and
- d. Procedures for monitoring changes in processing PII and implementing audits and reviews to ensure changes are made relevant to regulatory and legal requirements.

#### **PT-4 CONSENT**

Consent mechanisms ensure individuals have control over how their PII is processed and allows them to make informed decisions about collection and use of their data.

Individual State agencies shall provide clear information through Privacy Notices on how their PII will be processed and offer options for individuals to tailor or revoke their consent, and shall:

- a. Implement mechanisms for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate the individuals' informed decision-making;
- b. Allow individuals to give informed consent regarding the processing of their PII before its collection;
- c. Provide mechanisms to allow individuals to tailor processing permissions to selected elements of PII;
- d. Implement tools for individuals to revoke consent to the processing of their PII; and
- e. Use plain language and avoid using technical jargon to ensure individuals understand the risks and implications of giving consent.

#### **POLICY OWNER**

Secretary of Office of Information Technology (OIT)

#### **MATERIAL SUPERSEDED**

This is the first State of Alabama Personally Identifiable Information Processing and Transparency Policy. All State agencies and vendors of the State are required to comply with the current implemented version of this policy.



# PII Processing and Transparency Policy



PR-DS-P2

**Effective Date:**  
01/31/2025

**Date Approved:**  
01/15/2025

**Version:**  
1

**Page #:**  
4 of 5

## REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Initial Creation

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK



**PII Processing and Transparency Policy**



**PR-DS-P2**

**Effective Date:**  
01/31/2025

**Date Approved:**  
01/15/2025

**Version:**  
1

**Page #:**  
5 of 5

**APPROVED BY**

Signature	<i>Daniel Urquhart</i>
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

**REMAINDER OF PAGE LEFT INTENTIONALLY BLANK**