SOUTH CAROLINA
DEPARTMENT OF EDUCATION

TITLE OF POLICY: SC Personally Identifiable Information Processing and Transparency

SECTION: Information Security and Privacy

SUBSECTION: Data Protection and Privacy

POLICY NUMBER: 704.1

OFFICE OF RESPONSIBILITY: CISO

EFFECTIVE DATE: May 01, 2025

THE RELEVANT DEPARTMENT OF ADMINISTRATION POLICY IS ATTACHED. BELOW IS A SYNOPSIS OF THE POLICY CONTENTS:

1. Purpose and Scope

This policy is part of the South Carolina statewide information security framework and establishes requirements for the proper handling, processing, and protection of personally identifiable information (PII). It ensures that agencies manage personal data in a lawful, transparent, and accountable manner.

The policy applies to all state agencies and supports the broader information security and privacy program. Agencies must comply with applicable laws and regulations and may supplement this policy with organization-specific procedures to address operational needs.

2. Core Objective

The policy's primary objective is to ensure that agencies process PII responsibly and transparently in order to:

- Protect the privacy of individuals
- Ensure lawful and authorized data processing
- Promote transparency and accountability in data usage
- Reduce risks associated with misuse or unauthorized disclosure of personal information

3. Key Policy Requirements

A. Governance and Oversight (PT-1)

- Agencies must develop, document, and maintain policies and procedures governing PII processing and transparency.
- A designated official must oversee implementation and ongoing updates.
- Policies must align with applicable legal, regulatory, and organizational requirements.

B. Authority to Process PII (PT-2)

- Agencies must identify and document the legal authority that permits the collection and use of PII.
- Processing activities must be limited strictly to those authorized by applicable laws and regulations.

C. Purpose Specification and Limitation (PT-3)

- Agencies must define and document the specific purposes for which PII is collected and processed.
- These purposes must be communicated through public privacy notices.
    - PII must only be used in ways that are consistent with the stated purposes.
    - Changes to processing activities must be monitored and controlled to ensure continued compliance.

D. Consent (PT-4)

- Agencies must provide mechanisms for individuals to give informed consent before their PII is collected or processed.
- Consent processes must support clear and informed decision-making by individuals.

E. Privacy Notice and Transparency (PT-5)

- Agencies must provide clear, accessible privacy notices to individuals at the point of data collection and thereafter.
- Notices must be written in plain language and include:
    - The authority for collecting PII
    - The purposes for processing the information
    - Relevant details about how the information will be used

4. Security and Compliance

- Must comply with FERPA, state privacy laws, and the South Carolina Public Records Act.
- Content may be considered public record and is subject to audit or disclosure.
- This policy will be reviewed annually. Violations may result in disciplinary action or loss of access.

5. Related Policies:

- SC Risk Assessment Policy Draft (701.3)
- SC Access Control (702.4)
- SC Audit and Accountability Policy Draft (706.3)

Information Security and Privacy Policy – Personally Identifiable Information Processing and Transparency

Division of Information Security

May 01, 2025

Revision History

Version Number	Date	Author(s)	Description
2.0	May 1, 2025	Division of Information Security	Updated for SCDIS-200 v2.0

CONTENTS

1.0 INTRODUCTION

A. Purpose

The South Carolina Statewide Information Security Program (SC Infosec Program) consists of information security policies, standards and guidelines that establish a baseline information security framework to protect the information technology systems of South Carolina state government agencies[1].

Implementing the baseline framework is critical to the development of an agency information security and privacy program. An effective information security and privacy program continually improves the overall security posture for the state, as it integrates and matures toward support of the state and organizational mission, goals and objectives.

This *Personally Identifiable Information Processing and Transparency Policy* establishes requirements for properly managing and protecting personally identifiable information (PII).

B. Authority and Responsibilities

The organizational and functional responsibilities for the South Carolina Division of Information Security (DIS) and Agency are established in the SC Infosec Program's "Master Policy."

C. Scope

Organizations shall comply with the SC Infosec Program's policies, standards and guidelines. Implementation of the SC Infosec Program's policies, standards and guidelines is not meant or intended to replace, supersede or otherwise nullify agency compliance requirements identified in other applicable federal, state, local, agency or institutional regulations, policies or guidance. Likewise, compliance with the SC Infosec Program's policies, standards and guidelines does not convey compliance with other regulatory requirements agencies may have for information security.

Organizations may implement policies, standards and guidelines "as-is," but are encouraged to develop additional agency or institution-specific guidance to address unique components of their business operations.

[1] The term "Agency" will be used to refer to SC state government agencies as described in the SC Infosec Program's "Master Policy."

2.0 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY POLICY STATEMENTS

A. Policy and Procedures [PT-1]

NIST CSF Reference: GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03

1. Agencies shall develop, document and disseminate:
    a. A PII processing and transparency policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines.
    b. Procedures to facilitate the implementation of the *Personally Identifiable Information Processing and Transparency Policy* and the associated PII processing and transparency controls.
2. Agencies shall designate an official to manage the development, documentation and dissemination of the PII processing and transparency policy and procedures.
3. Agencies shall review and update the current PII processing and transparency policy and procedures at defined frequencies and following defined events.

B. Authority to Process Personally Identifiable Information [PT-2]

NIST CSF Reference: GV.OC-03

1. Agencies shall determine and document the authority permitting the processing of PII.
2. Agencies shall restrict the processing of PII to only that which is authorized.

C. Personally Identifiable Information Processing Purposes [PT-3]

NIST CSF Reference: GV.OC-03

1. Agencies shall identify and document the purpose(s) for processing PII.
2. Agencies shall describe the purpose(s) in the public privacy notices and policies of the organization.
3. Agencies shall restrict the processing of PII to only that which is compatible with the identified purpose(s).
4. Agencies shall monitor changes in processing PII and implement mechanisms to ensure changes are made in accordance with defined requirements.

D. Consent [PT-4]

NIST CSF Reference: GV.OC-03

Agencies shall implement defined tools or mechanisms for individuals to consent to the processing of their PII prior to its collection to facilitate individuals' informed decision-making.

E. Privacy Notice [PT-5]

NIST CSF Reference: GV.OC-03

Agencies shall provide notice to individuals about the processing of PII that:

1. Is available to individuals upon first interacting with an agency, and subsequently.
2. Is clear and easy-to-understand, expressing information about PII processing in plain language.
3. Identifies the authority authorizing the processing of PII.
4. Identifies the purposes for which PII is to be processed.
5. Includes agency-defined information as required.