State of Maryland

STANDARD

PI/PII & TRANSPARENCY

Document No.	Last Updated	Prepared By
MD-STD-315-PT-02	6/30/2026	DOIT OSM

The protection of Personal Information (PI) / Personally Identifiable Information (PII) and transparency are crucial to fostering trust, enforcing strict access controls, and complying with privacy laws.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to process PI / PII responsibly, maintain transparency, and comply with privacy regulations.
	This standard addresses privacy controls related to the collection, use, maintenance, disclosure, and disposal of PI/PII.
	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as "agencies."
	This standard is part of a broader policy suite. Refer to MD-POL-100 Cybersecurity & Governance Policy, Appendix C for a list of related policies and standards.
	This standard has been developed using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 Moderate Baseline[1] and State-specific organizationally defined parameters. Agencies may be required to deviate from this baseline when State statute, executive orders, or applicable regulations establish a conflicting requirement that precludes compliance.
	This document is approved for public distribution and may be shared with external stakeholders, partners, and regulatory bodies. It reflects the State's commitment to transparency, compliance, and operational excellence. Unauthorized modifications or misrepresentation of this document are strictly prohibited.

[1] NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

FOREWORD

Agencies that use Department of Information Technology (DoIT) managed services automatically receive, or *inherit*, the compliance those services already meet, reducing duplicative work and accelerating their overall compliance efforts. These centrally governed services are built with robust control frameworks that automatically extend to participating agencies. By leveraging these offerings, agencies not only align with key operational and security standards but also benefit from pre-configured environments, continuous monitoring, and policy enforcement mechanisms maintained by DoIT. Agencies are encouraged to leverage these services to accelerate readiness, gain cost efficiency, and simplify compliance efforts, which allows agencies to focus more fully on mission delivery. Agencies should review the scope of each managed service to understand which standards are inherited and where additional agency-specific controls may still be required.

GUIDANCE AND ENFORCEABILITY

This Standard utilizes informational call-out boxes to provide additional context or elaborate on key topics. While these boxes primarily serve an informational purpose, any directives or mandated actions contained within them are authoritative and carry the same enforceability as the core requirements of this document. For the purposes of this document, the term “shall” denotes a mandatory requirement. Terms such as “where feasible,” “encouraged,” or similar phrasing indicate recommended practices that reflect organizational preference but are not enforceable requirements at this time. This Standard applies to both PI and PII except where only one is specifically noted.

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026
2.0	Added Sections 315-9 and 315-10; Modifications to 315-2, 315-3, 315-4. And 315-5.	Miheer Khona	06/30/2026

STANDARDS

315 State Strategy

This Standard establishes a baseline of privacy and transparency practices that each agency must implement to comply with State cybersecurity and privacy policies. Each agency shall designate specific personnel with IT responsibilities to ensure their effective implementation.

315-1 Develop Agency-Level Procedures (PT-1)

In alignment with this Standard, develop and document agency-level privacy protection and transparency procedures. Agencies must disseminate the procedures to agency personnel with information technology (IT) security responsibilities. Agencies must review, and if needed, update the procedures as deemed appropriate by the agency based on changes and risk at least every **3 years**. At a minimum, the procedures must address purpose, scope, roles and responsibilities, and guidelines.

315-2 Establish Authority to Process (PT-2)

Document the authority that permits the processing of PI and PII and ensure that it is processed only as explicitly authorized.

315-3 Define Processing Purposes (PT-3)

Document the purpose(s) for processing PI/PII. Describe the purpose(s) in the public privacy notices and policies of the organization. Restrict the processing of PI/PII to that which is compatible with the identified purpose(s). Monitor changes in processing, requiring review and approval through the agency's formal change control process and privacy risk assessment.

PI/PII may be used only for purposes originally disclosed unless otherwise authorized by law. Ensure only those staff with a need to know are provided with authorized access. Third party contractors must be bound by confidentiality obligations at least as restrictive as those set forth in Attachment Y: Data Use Agreement (DUA) to process PI.

315-4 Obtain Consent (PT-4)

Agencies must notify individuals of the purpose, legal authority, and intended use of their PI/PII and obtain consent prior to collection. Limit use of PI/PII to the specific purpose for which an individual consented. Doing so respects the individual's privacy and control overuse of their PI/PII.

Implement State-approved tools or mechanisms that enable individuals to provide consent for the processing of their PI/PII prior to collection.

315-5 Privacy Notice and Required Disclosures Prior to Collecting or Sharing PI/PII (PT-5)

Privacy Notice

A Privacy Notice is a public facing page on the agency's website that informs the public about an agency's practices in the handling of PI/PII entrusted to the agency. The Privacy Notice must follow the practices listed below:

- Be clear and easy-to-understand, expressing information about information processing in plain language;
- Identify the authority that authorizes the collection and processing of PI/PII;
- Identify the purposes for which PI/PII is to be processed; and,
- Describe the data practices used.

Required notification prior to collection or sharing of PI/PII

Agencies must provide notification to individuals prior to obtaining PI/PII from them or sharing their PI/PII with a third party. The notifications must include:

- At or before the time of collection of PI/PII:
    - That PI/PII is being collected and for what purpose;
    - The legal authority requiring the collection of PI/PII;
    - Whether the provision of the PI/PII is voluntary; and
    - Instructions on how to receive information, which shall be provided upon request of the individual if allowed by law, about the:
        - Types of PI/PII collected about the individual;
        - Sources from which the PI/PII was collected.
- At or before the time of an agency's sharing of PI/PII:
    - The specific PI/PII shared and its source,
    - The purpose for which the PI/PII is shared and how it will be used.
    - The circumstances in which the PI/PII will be shared;
    - The recipients of the shared PI/PII;
    - The legal authority for the sharing of PI/PII; and
    - Any rights the individual may have to:
        - Review the PI/PII shared; or
        - Decline the agency's sharing of PI/PII.

Consult with your Agency Privacy Officer (APO) and Assistant Attorney General (AAG) to review applicable State privacy directives to determine how the agency provides the above notices (e.g.,

included with forms or applications that collect PI/PII, posted at the point of collection.) *Note: If the agency collects information on behalf of a federal agency or manages federally regulated data, consult the APO and AAG to determine if specific federal Privacy Act statements are required under an applicable federal data-sharing agreement.*

315-6 System of Records Notice (PT-6)

While the State is exempt from the Privacy Act of 1974, the MD Data Privacy Executive Order 01.01.2021.10 and SCPO require conformance with the Fair Information Privacy Practices (FIPPs). Under FIPPs, Systems of Records Notices are not required for States.

Fair Information Practices Principles (FIPPS)

The Fair Information Practice Principles (FIPPs) are a set of internationally recognized privacy principles based upon the Privacy Act of 1974 that inform privacy policies and practices within government and the private sector. The SCPO adopted the following principles, in conjunction with State and applicable federal law, to promote individuals' privacy rights and data protection:

Purpose Specification - Agencies should specifically articulate the authority that permits the collection of PI/PII. The purpose(s) for which PI/PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PI/PII was collected (or other purposes compatible with the original collection purpose).

Individual Participation - To the extent practicable, agencies should involve the individual in the process of using PI/PII and seek individual consent for the collection, use, dissemination, and maintenance of PI/PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PI/PII.

Collection Limitation/Data Minimization – PI/PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PI/PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

Use Limitation - PI/PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law.

Data Quality/Integrity – PI/PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

Security/Safeguards – Agencies should institute reasonable security safeguards to protect PI/PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

Openness/Transparency – To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PI/PII. Agencies should publish their privacy policies and Privacy Notice publicly and provide contact information for data corrections and complaints.

Accountability/Audit – Agency personnel and contractors are accountable for complying with measures implementing FIPPs, for providing training to all employees and contractors who use PI/PII, and for auditing the use and storage of PI/PII.

*Source: Department of Homeland Security FIPPS at Work Fact Sheet

315-7 Address Specific Categories of PII/PI (PT-7)

Apply security controls for all categories of PI/PII commensurate with assessed risk.

Zero Trust Architecture

Where feasible apply the Zero Trust Architecture (ZTA) to control access to PI/PII. Examples include: a) Enhanced Identity Governance (EIG) - Strict access controls and authentication mechanisms for PI/PII, reducing unauthorized access risks; b) Software-Defined Networking (SDN) – Limit access to PI/PII by dynamically managing network flows and applying identity and context-aware policies, ensuring secure and adaptive connectivity; c) Micro-segmentation – Divide networks into smaller segments to restrict lateral movement, ensuring PI/PII is only accessible within designated zones; and d) Secure Access Service Edge (SASE) – Integrate security functions like identity verification and encryption to protect PI/PII across cloud environments. Architecture updates should align with NIST SP 800-207, State EA, and CISA ZTA maturity model.

PT-7(1): When a system processes Social Security numbers (SSNs): a) Eliminate unnecessary collection, maintenance, and use of SSNs, and explore alternatives to their use as a personal identifier; b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN; and c) Inform any individual who is asked to disclose their SSN whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is requested, and what uses will be made of it.

PT-7(2): Prohibit the processing of information describing an individual's exercise of First Amendment rights unless such processing is expressly authorized by statute, authorized by the individual, or necessary and within the scope of an authorized law-enforcement activity.

315-8 Meet Computer Matching Requirements (PT-8)

When the State processes information for the purpose of conducting a matching program:

- Consult with the APO, and if required by a federal agency, review the appropriate federal Data Integrity Board, to conduct the matching program;
- Develop and enter into a computer matching agreement;
- Independently verify the information produced by the matching program before taking adverse action against an individual; and
- Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

Computer Matching Program

Under the Computer Matching and Privacy Protection Act of 1988, a computer matching program is defined as: "The computerized comparison of two or more automated systems of records, or a system of records with non-federal records, for the purpose of establishing or verifying eligibility or compliance for federal benefit programs." This includes matching data such as SSNs, income, or employment status across agencies like the Social Security Administration (SSA), Department of Health and Human Services (HHS), or Department of Homeland Security (DHS).

315-9 Prohibit Sale of Personal Information and Protect Personal Record Information

The State does not sell PI/PII. The Maryland Data Privacy and Protection Act of 2026 expanded the definition of "personal information" to include "sensitive data" to protect Data Subjects from potential harm to their privacy resulting from the release of their sensitive data without consent. Third parties authorized to process PI/PII to perform a contracted service for the State are prohibited from redisclosing or monetizing PI/PII without explicit Data Subject consent. Further, consistent application of FIPPS, particularly for PI/PII collection, retention, and disclosure, is the most effective way for agencies to prevent the resale or redisclosure of PI/PII as required by Md. State Govt. Article, § 10-1702.

315-10 Execute Data Use Agreements with Third-Party Processors

To protect PI/PII from unauthorized use or redisclosure by contractors or third parties that process PI/PII on behalf of the agency, agencies must use the *Office of State Procurement Attachment Y: Data Use Agreement,* or ensure that the contract entered into with a contractor or other third party contains no less restrictive privacy preserving measures than the Data Use Agreement. Contracts must contain:

- Purpose Limitation & Data Minimization
- Legal Disclosure & State Notification Protocol
- Prohibition on Data Monetization
- Marketing & Behavioral Advertising Restrictions
- Sub-Processor Oversight & Accountability Guidelines

The following table consolidates the leading industry best practices and authoritative guidelines related to this standard.

GUIDELINES

ID			
CSF Tools	Cyber Security Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools (LINK)*
NIST Privacy Framework	NIST Privacy Framework	This is a tool designed to help organizations identify and manage privacy risks while building innovative products and services.	*csf.tools (LINK)*
NIST SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information	This guide assists federal agencies in safeguarding the confidentiality of PI/PII within information systems, aligning security practices with privacy principles.	*csf.tools (LINK)*
OMB 17-12 Memorandum	Preparing for and Responding to a Breach of Personally Identifiable Information (PI/PII)	This document provides federal guidelines for preparing for and Responding to a Breach of Personally Identifiable Information.	*csf.tools (LINK)*
Maryland General Provisions Article, §§ 4-101 through 4-601	Maryland Public Information Act	The Maryland Public Information Act (MPIA) requires state and local government agencies to provide public access to government records unless a specific exemption applies. It balances transparency with privacy by allowing access to most records while protecting sensitive information such as personal data, law-enforcement materials, and confidential business information.	*MPIA (LINK)*

Maryland State Government Article, §10-1301	Protection of Information by Government Agencies (PIGA)	Requires government agencies to implement reasonable security measures to protect personal information they collect and maintain from unauthorized access, use, or disclosure.	*MD PIGA (LINK)*
Maryland State Government Article § 10-1702	Maryland Online Data Protection Act	Requires procedures to prevent or dissuade third party sale or redisclosure of personal records and geolocation data made available by the State.	*MD , State Government Article § 10-1702 (LINK)*
Maryland Data Privacy Executive Order 01.01.2021.10	EXECUTIVE ORDER 01.01.2021.10 Maryland Data Privacy	State units have a responsibility to protect the privacy of PII in State systems while facilitating appropriate data sharing and analyses	*MD EO 01.01.2021.10 (LINK)*
Attachment "Y"	Data Use Agreement	Maryland Data Use Agreement used for third party contractors ("Processors") that process PI/PII under contract with the State. If other than Attachment Y is used, the agreed upon data protections must be as protective as Attachment Y.	*See your procurement officer for the Data Use Agreement, known as "Attachment Y."*

DEFINITIONS

Each unique term used in this standard is defined in the **State of Maryland Cybersecurity & Privacy Glossary**.

COMPLIANCE CHECKLIST

ID		mpliance
315-1	**Develop Agency-Level Procedures (PT-1)**	☐ Yes ☐ No
315-2	**Establish Authority to Process PI/PII (PT-2)**	☐ Yes ☐ No
315-3	**Define Processing Purposes (PT-3)**	☐ Yes ☐ No
315-4	**Obtain Consent (PT-4)**	☐ Yes ☐ No
315-5	**Provide Privacy Notice and Required Disclosures Prior to Collecting or Sharing PI/PII (PT-5)**	☐ Yes ☐ No
315-6	**System of Records Notice (PT-6)**	☐ N/A
315-7	**Address Specific Categories of PI/PII (PT-7)**	☐ Yes ☐ No
315-8	**Meet Computer Matching Requirements (PT-8)**	☐ Yes ☐ No
315-9	**Prohibit Agency Sale of Personal Information and Protect Personal Record Information (PT-9)**	☐ Yes ☐ No
315-10	**Execute Data Use Agreements with Third-Party Processors (PT-10)**	☐ Yes ☐ No

Note: When assessing the implementation and effectiveness of the security and privacy controls outlined in this standard, DoIT recommends the use of NIST SP 800-53A Rev. 5, to perform evaluations in a manner that is evidence-based, repeatable, and aligned with the system's documented security posture.