State of Maryland

STANDARD

PII & TRANSPARENCY

Document No.	Last Updated	Prepared By
MD-STD-315-PT-01	02/18/2026	DOIT OSM

The protection of Personally Identifiable Information (PII) and transparency is 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 PII responsibly, maintain transparency, and comply with privacy regulations.
Scope	This standard addresses privacy controls related to the collection, use, maintenance, disclosure, and disposal of PII.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as "agencies."
Related Policy	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.
Baseline	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.
Distribution	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, such as hosting platforms, identity management, and network infrastructure, 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, simplify compliance efforts, and allow agencies to focus more fully on mission delivery, knowing that foundational requirements are already in place. 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

Throughout this document, informational call-out boxes are utilized 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.

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026

STANDARDS

315 State Strategy

These standards establish 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 the effective implementation of these standards.

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 PII (PT-2)

In coordination with the State Chief Privacy Officer (SCPO), determine and document the agency-level authority that permits the processing of PII, and ensure that PII is processed only as explicitly authorized.

315-3 Define PII Processing Purposes (PT-3)

Identify and document the agency-defined purpose(s) for processing PII. Describe the purpose(s) in the public privacy notices and policies of the organization. Restrict the processing of 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.

315-4 Obtain Consent (PT-4)

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

315-5 Provide Privacy Notice (PT-5)

Provide notice to individuals about the processing of PII that:

- Is available to individuals upon first interacting with the agency, and subsequently via the privacy notice published on the State website;

- Is clear and easy-to-understand, expressing information about PII processing in plain language;
- Identifies the authority that authorizes the processing of PII; and
- Identifies the purposes for which PII is to be processed.

Consult with the SCPO on privacy notice templates to ensure uniform language and formatting across agencies.

PT-5(2): Consult the SCPO and review the Office of Management and Budget (OMB) Circular A-108 to determine if Privacy Act statements must be included on forms that collect information, particularly if it will be maintained in a Privacy Act system of records or provide Privacy Act statements on separate forms that can be retained by individuals.

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

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

Fair Information Privacy Practices

The FIPPs[2] are a foundational framework for privacy and data protection, originally developed in the 1970s and widely adopted across government and industry. They guide how organizations should collect, use, and manage personal information responsibly using the following principles: a) Transparency (Notice); b) Individual Participation (Access); c) Purpose Specification; d) Data Minimization; e) Use Limitation; f) Security Safeguards; g) Accountability; h) Data Quality; and i) Integrity.

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

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

[2] Fair Information Practice Principles (FIPPs) | FPC.gov

Zero Trust Architecture
Where feasible apply the Zero Trust Architecture (ZTA) to control access to PII. Examples include: a) Enhanced Identity Governance (EIG) - Strict access controls and authentication mechanisms for PII, reducing unauthorized access risks; b) Software-Defined Networking (SDN) – Limit access to 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 PII is only accessible within designated zones; and d) Secure Access Service Edge (SASE) – Integrate security functions like identity verification and encryption to protect PII across cloud environments. Architecture updates should align with NIST SP 800-207 and State EA 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:

- Obtain approval from the SCPO and, when required by a federal agency, 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).

GUIDELINES

ID	Title	Description	Source
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 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 (PII)	This document provides federal guidelines for preparing for and Responding to a Breach of Personally Identifiable Information.	*csf.tools (LINK)*

DEFINITIONS

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

COMPLIANCE CHECKLIST

ID	Standard	Compliance
315-1	**Develop Agency-Level Procedures (PS-1)**	☐ Yes ☐ No
315-2	**Establish Authority to Process PII (PT-2)**	☐ Yes ☐ No
315-3	**Define PII Processing Purposes (PT-3)**	☐ Yes ☐ No
315-4	**Obtain Consent (PT-4)**	☐ Yes ☐ No
315-5	**Provide Privacy Notice (PT-5)**	☐ Yes ☐ No
315-6	**Provide System of Records Notice (PT-6)**	☐ Yes ☐ No
315-7	**Address Specific Categories of PII (PT-7)**	☐ Yes ☐ No
315-8	**Meet Computer Matching Requirements (PT-8)**	☐ 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.