STANDARD OPERATING PROCEDURES

DOIT-SOP-415-PT

Last Updated: 06/25/2026

PURPOSE

The Standard Operating Procedures (SOP) procedures implement cybersecurity and privacy standards required by MD-STD-315 PII & Transparency Standard. [MD Code, State Government, § 10-1702]

IMPORTANT: Any change to this SOP must be synchronized with the MD-STD-315 PII & Transparency Standard to ensure conformance. This SOP must be reviewed at least **every three years** and updated as needed to reflect any changes to the standards.

SCOPE

The procedures outlined in this SOP are specific to the following organizations within the State of Maryland:

Organization	Description
Maryland Insurance Administration (MIA)	The MIA is the state agency that regulates insurance in Maryland.
And all contractors, vendors, processors, and third parties with access to personal information on behalf of the State.	Salesforce, NAIC, MD AdvoKit, Carasoft & Box

ROLES & RESPONSIBILITIES

The procedures outlined in this SOP are assigned to the following individuals:

Name	Role	Responsibilities
H. Brent Matthewson Jr.	Agency Privacy Officer (APO)	PT-9.01, and PT-10.01
H. Brent Matthewson Jr.	Agency Data Owner (DO)	PT-9.01.02
Anthonia Chuku	Procurement Contract Monitor (PCM) and Procurement Officer (PO)	PT-9.01, and PT-10.01
Gui Bekaert	Information Security (Infosec)	PT-9.01
Craig Ey, Joe Sviatko, Dhaivat Maharaja	Agency Public Information Officer (PIO) or Communications Officer (CO), Management Information Systems (MIS)	PT-9.01.02

PROCEDURES

PT-9.01: Agency Prohibition on the Sale of Personal Information (315-9)

● The Procurement Officer, Contract Monitor and APO after legal sufficiency review by the OAG unit for MIA ensure agreements disallow the sale of personal information that has been collected by the Agency or Vendors on behalf of the State, including strictly restricting third parties authorized to process PI from the sale/reselling, licensing, renting, monetizing, or otherwise deriving commercial value from State-provided personal data. [MD Code, State Government, § 10-1702]
● Infosec or designee assigned to perform third-party risk assessments includes in the audit that the third parties do not repurpose PI for secondary, non-contracted uses, including but not limited to building commercial profiles, targeted/behavioral advertising, or training proprietary machine learning/AI models.
● Procurement Officer ensures the execution Attachment Y: Data Use Agreement to document restrictions on third parties from redisclosing PI to any external entity unless expressly required to fulfill the contracted service, as explicitly mandated by law, or authorized by the Data Subject.
● Infosec identifies and classifies all systems containing PI.

PT-9.01.02: Implement FIPPs to Protect Personal Records Made Available Pursuant to a PIA (315-9)

● When collecting information, data requestors implement FIPPS to ensure only the minimum amount of personal information necessary to meet a legitimate government purpose is requested. Additionally, data users ensure personal information is used or shared in line with the specified purposes for which the Data Subject consented and provided the information.
● The MIS and Agency Data Officer ensures Agency compliance with the Maryland Archives retention schedule requirements and Office of Enterprise Data policies related to records retention.
● The MIS and Agency Data Officer prioritizes the sharing of fully de-identified or aggregate data whenever possible to mitigate the risk of unauthorized redisclosure of PI.
● The MIS and Agency Data Officer makes the determination of data minimization at the field level, not the record level. An entire record should not be withheld if specific identifying information can be removed.
● The MIS and Agency Data Officer document in the response to a requestor any minimization of identifying fields in the record and cite Standard 315 as the basis for the minimization.
● Additionally, bulk information requests are discouraged, but if legally allowed, the MIS and Agency Data Officer, or designees, will confirm that only allowable personal record information is released in accordance with MD Code, State Government, § 10-1702.

PT-10.01: Data Use Agreements & Third-Party Processors (315-11)

- The Procurement Officer, Contract Monitor, and APO include the State approved Data Use Agreement into all third-party contracts, explicitly prohibiting the sale, monetization, or use of PI for targeted marketing. They additionally enforce strict parameters, so vendors only access necessary data fields, utilize encrypted data transfers, and mandate the secure destruction of PI upon contract termination. See Attachment “Y”.

- The Procurement Officer, Contract Monitor, and APO require third parties to provide an updated "Authorized Sub-Processor List" upon request and immediately notify the State of any legal subpoenas or government requests for PI.

- The Procurement Officer reviews Contractual Agreements in which PI is processed to ensure the agreement contains:
    - Purpose Limitation & Data Minimization
    - Legal Disclosure & State Notification Protocol
    - Prohibition on Data Monetization
    - Contractor requirement to notify the State of any law enforcement, judicial and/or government requests of the Contractor for Personal Information, including Sensitive Data,
    - Marketing & Behavioral Advertising Restrictions
    - A list of Sub-Processors and defined Contractor oversight & accountability
    - Data elements to be Processed pursuant to the contract