Board of Directors

Audit Committee Meeting

Click to view online: https://www.youtube.com/watch?v=eTf5652v9l0

October 22, 2026

9:00 a.m.

BOARD MEMBERS:

Moalie Jose, P.E., *Chair, Audit Committee*
Sean L. Coleman, Esq.
Rebecca L. Flora, AICP
James H. Johnson Jr., Ph.D., P.E.
Shelley L. Heller
Charles C. Glass, Ph.D., P.E.

Agenda

Call to Order	Moalie Jose
Approval of Minutes – May 21, 2026	Moalie Jose
SB& Company FY26 Audit	Monique Booker
Internal Audit Report	Ryan Dowdell
PI/PII Policy	Jeff Tosi
Old/New Business	Moalie Jose
Adjournment	Moalie Jose

Policy #: IT 1.03
Policy Category: IT
Department Responsible: Administration
Original Adoption Date: 10/29/2026
Board of Directors Approval: 10/26/2026
Last Edit: 10/26/2026

PERSONAL INFORMATION & PERSONALLY IDENTIFIABLE INFORMATION & TRANSPARENCY POLICY

I. Scope & Purpose

It is the policy of the Maryland Environmental Service (Agency) to protect Personal Information (PI) and Personally Identifiable Information (PII) prevent the unauthorized sale and disclosure or redisclosure of personal records, and to the maximum extent reasonable to be open and transparent about the collection, use, dissemination, and maintenance of PI/PII.

This policy is developed in accordance with State Government Article § 10-1702 and the Maryland Department of Information Technology (DoIT) Standard MD-STD-315-PT-02.

II. Definitions

A. "Personal Information (PI)", "Personally Identifiable Information (PII)", and "Sensitive Data" have the same meanings as defined in the Cybersecurity and Privacy Glossary published by the Maryland Department of Information Technology (DoIT Glossary), as amended from time to time. It is the intention of the Agency to adopt and apply the most current version of the definitions in the DoIT Glossary, as amended. At the time of adoption of this Policy, the current definitions are as follows:

1. "Personal Information (PI)" means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements: a Social Security number, an Individual Taxpayer Identification number, a passport number, or other identification number issued by the federal government; a driver's license number or State identification card number; a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account; a username or email address in combination with a password or

security question and answer that permits access to an individual's email account; or Sensitive Data.

2. “Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual’s identity, such as name, social security number, biometric data records. either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother’s maiden name, etc.).

B. “Sensitive Data” means data revealing racial or ethnic origin, religious beliefs, consumer health data, sex life, sexual orientation, status as transgender or nonbinary, national origin, citizenship or immigration status, genetic data or biometric data, personal data of an individual that the controller (or data owner) knows or has reason to know is a child, or Precise Geolocation. Sensitive data includes data inferred by a controller based on personal data that, alone or in combination with other data, is used to describe any of the sensitive data elements. This data is subcategory of personal data which falls under confidential data (Data Classification Level 3) in accordance with the State Data Classification Policy.

C. “Third-Party Processor” means any external contractor, vendor, or entity authorized by the Agency to process PI/PII to perform a contracted service.

II. SCOPE AND AUTHORITY TO PROCESS

A. This policy applies to all PI/PII collected, maintained, and disposed of by the Agency.

B. The Agency restricts the collection, processing, and maintenance of PI/PII to the minimum amount necessary to accomplish legitimate, explicitly authorized purposes.

C. The Agency’s processing of PI/PII is strictly limited to employment administration, employee and dependent health and emergency contact information, building and security access, necessary procurement and contracting records, and necessary customer information for any of the Agency’s operations. The Agency does not collect, capture, or maintain public consumer databases or public geolocation data that is not directly germane to operations.

III. ROLES AND RESPONSIBILITIES

A. The Managing Director for Administration, or the Managing Director's designee, shall serve as the primary point of contact for compliance with and the periodic review of this policy.

B. The Human Resources Division is responsible for safeguarding employee and dependent PI/PII, ensuring only individuals with a legitimate purpose are authorized access to any PI/PII.

C. The Procurement Division is responsible for ensuring all third-party processors are bound by appropriate confidentiality and data use protections and obligations.

D. The MES Information Technology Division is responsible for providing secure, reliable, and innovative technology services that support MES business operations. The division is responsible for IT governance, cybersecurity, network and system infrastructure, enterprise applications, data protection, technical support, asset management, and technology strategy to ensure the confidentiality, integrity, and availability of MES information systems and services.

IV. PRIVACY CONTROLS AND OPERATING GUIDELINES

A. Prohibition on the Sale of PI/PII: The Agency strictly prohibits the sale, monetization, or commercial exploitation of any PI/PII, sensitive data, or personal records.

B. Data Minimization: PI/PII shall be collected and stored only if the data is directly related to and necessary for accomplishing the specific purpose for which it is intended. Subsequent use of this data is restricted to the original purpose for which it was collected.

C. Privacy Notices: The Agency shall provide clear and accessible privacy notices to individuals regarding the collection, use, maintenance, sharing, and disposal of PI/PII, as required by applicable laws, regulations, executive directives, or contractual obligations.

D. Sensitive Categories: The Agency shall ensure that the collection, use, maintenance, sharing, or disposal of sensitive categories of PI/PII, including but not limited to Social Security numbers (SSNs) or other uniquely identifying data elements, is:

1. Authorized and documented in accordance with applicable laws,

regulations, executive directives, or contractual obligations;

2. Limited to what is necessary to accomplish authorized business purposes; and

3. Protected using appropriate administrative, technical, and physical safeguards commensurate with the sensitivity of the PI/PII.

E. Data Use Agreements with Third-Party Processors: To protect PI/PII from unauthorized use or redisclosure by contractors or third-party processors, the Agency shall incorporate protective clauses into its vendor contracts. Any contract granting a third-party access to Agency PI/PII must contain privacy-preserving measures no less restrictive than the Office of State Procurement Attachment Y: Data Use Agreement. At a minimum, these contracts must enforce:

1. Purpose Limitation & Data Minimization

2. Legal Disclosure and State Notification Protocol

3. A Prohibition on Data Monetization

4. Sub-Processor Oversight & Accountability Guidelines

5. Marketing and Behavioral Advertising Restrictions

F. Public Information Act Requests: The Agency shall provide a clear and accessible notice to any person who submits a public information act request that any portion of the records that contains PI/PII (1) may be denied inspection in accordance with General Provisions Article Title 4, Subtitle 3, and (2) may not be sold or redisclosed.

V. PERIODIC REVIEWS AND UPDATES

A. Consistent with DoIT Standard MD-STD-315-PT-02, the Managing Director of Administration, or their designee, shall review and update this Policy at least every three years.

B. Updates shall be based on changes to processing practices, changes in state law or regulations, privacy risk assessments, or any other factors that may impact the security and privacy of PI/PII.

VI. Related Policy and Procedure Links

- HR Policy #1.17 – Personnel Files

VII. Revision History

Version	Date of Change	Section	Description of Change
.001	10/29/2026	Full Document	Initial Adoption of new policy