DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

Data Protection and Privacy Policy

Distribution Statement: 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.

TABLE OF CONTENTS

CHANGE RECORD

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

State of Maryland

DATA PROTECTION & PRIVACY POLICY

MD-POL-205-01	Last Updated: 02/18/2026

100 INTRODUCTION

Purpose:	This policy establishes requirements for safeguarding State data throughout its lifecycle and managing privacy risks in alignment with State and regulatory expectations.
Scope:	This policy addresses all State data, data types and data sets generated, received, stored, processed, or transmitted across State IT, whether the data is hosted on the State network or by a third-party provider.
Authorization:	This policy is authorized by State Finance & Procurement Article (SF&P) § 3.5-303 and § 3.5-2A-04.
Applicability:	This policy applies to all "units of State government" (as that term is defined in SF&P 3.5-101(g)), hereafter referred to as “agencies.”
Superseded Policy:	The full policy suite outlined in MD-POL-100 Cybersecurity & Governance Policy, Appendix C supersedes the State of Maryland Information Technology Security Manual Version 1.2, June 28, 2019.
Waivers:	Refer to the MD-POL-100 Cybersecurity Governance Policy guidance on exception requests and waivers related to this policy.
Stakeholder Roles:	**Department of IT (DoIT) -** The Department responsible for developing, maintaining, revising, and enforcing information technology policies, procedures, and standards.
	State Chief Information Security Officer (SCISO) - The appointed individual responsible for overseeing the State's cybersecurity strategy and ensuring the protection of its information systems.
	State Chief Privacy Officer (SCPO) - The individual responsible for supporting agencies in the development and implementation of effective privacy programs, developing privacy policies, and promoting compliance with data protection best practices.

	State Chief Data Officer (SCDO) - An individual appointed by the Governor to provide leadership in data governance and management across State government. The SCDO oversees standardization, collaboration, and ethical data practices while promoting effective data sharing. This role is responsible for directing, coordinating, and implementing the Statewide data strategy and policy.
	Executive Branch Secretaries, Executive Directors, and Administrators (or equivalent) – The individuals who oversee specific departments and agencies responsible for ensuring the implementation of this policy and any related standards for their respective agencies.
	IT Managers - Any staff with the responsibility for procuring or operating IT systems and equipment within an agency.
	Information Security Officers (ISO) – The individuals assigned to provide agencies with security expertise, guidance, and resources to assist agencies in meeting State and Federal cybersecurity compliance requirements.
	Information User (hereafter referred to simply as "user") - Any person who interacts with a State computer system, software application, or network service to include State employees, contractors, vendors, third-party providers.
Stakeholder Responsibilities:	Following the policy statements in each area, a RACI matrix is provided to clearly address responsibility for each policy statement as follows:
	[R] Responsible: The person or people within each agency who are tasked with completing the work.

	[A] Accountable: The person or people within each agency who authorize and assign the work and validate that the work is completed.
	[C] Consulted: The person or people within each agency whose input is sought during the completion of the task.
	[I] Informed: The person or people within each agency who need to be kept up to date on the progress or completion of the task.

All requirements in this policy remain in effect unless an applicable State Statute or Executive Order establishes a conflicting requirement that precludes compliance.

200 POLICY

The following sections detail the State's data protection and privacy policy outlining the activities needed to protect data from both internal and external threats.

200.1 DATA IDENTIFICATION

200.1.1 Data Identification and Classification: All agencies shall identify and classify State data within their purview in accordance with the State Data Classification Policy as directed by the Office of Enterprise Data (OED) State Chief Data Officer (SCDO), State Chief Information Security Officer (SCISO), State Chief Privacy Officer (SCPO), and Agency Data Officers (ADO), and State data governance policy and guidelines. Where feasible, agencies shall use automated means for data discovery, data labeling and tagging.

200.1.2 Privacy Analysis: All agencies shall determine which systems within their purview process personal information defined by the State as confidential information (Data Classification Level 3) by completing a Privacy Threshold Analysis (PTA), and where required, a Privacy Impact Assessment (PIA) as directed by the SCPO and in alignment with the State privacy procedures. These assessments shall be reviewed and updated upon significant changes to system, data, or processing.

200.1.3 Regulatory Requirements: All agencies shall determine which systems within their purview process regulated data (e.g., FTI, PCI DSS, HIPAA) that have cybersecurity compliance requirements. It is incumbent upon each agency to implement the regulatory requirements as part of their agency-level procedures. In the event that regulatory requirements are more stringent than State cybersecurity policy or standards, the regulatory requirements take precedence.

Table 1 RACI Matrix – Data Identification

	DOIT	SCISO/ SCDO/SCPO	Secretaries/ Directors	IT Managers	ISOs
Data Identification & Classification	I	C	A	R	I
Privacy Impact Analysis (PIA)	I	C	A	R	I
Regulatory Requirements	I	C	A	R	I

[R] Responsible, [A] Accountable, [C] Consulted, [I] Informed

200.2 DATA PROTECTION

All agencies shall protect data to preserve the confidentiality, integrity and availability (CIA) of that data.

200.2.1 Data at Rest: Non-public data (Data Classification Level 2 or above) that is housed digitally on computer data storage shall be encrypted. Applicable regulations may require specific forms of encryption for data at rest. Deploy encryption following the encryption standards defined by MD-STD-318 SC, Section 318-6, incorporating cryptographic agility, and protection of encryption keys (i.e., secrets are not hard coded and are rotated on a regular basis) or as required by regulatory requirements if they are more stringent.

200.2.2 Data in Transit: Non-public data (Data Classification Level 2 or above) that is being transferred between locations over the State network or the internet shall be encrypted. Applicable regulations may require specific forms of encryption for data in transit. Deploy encryption following the encryption standards defined by MD-STD-318 SC, Section 318-6, incorporating cryptographic agility, and protection of encryption keys (i.e., secrets are not hard coded and are rotated on a regular basis) or as required by regulatory requirements if they are more stringent.

200.2.3 Data in Use: Applications shall be securely designed to protect State data through enforced access controls and, where feasible, data masking to obfuscate non-public information during processing. Privacy-enhancing technology shall be used when practicable to protect personal information while sharing pertinent information .

200.2.4 Data Availability: Adequate capacity shall be allocated (e.g., internet bandwidth, storage, processing power, data management tools and security measures) to maintain availability of State data in accordance with business continuity and disaster recovery requirements.

200.2.5 Data Loss Prevention: Protections shall be implemented to prevent unauthorized disclosure or exfiltration of State data, including personal or restricted information, using

mechanisms such as boundary protection, information flow enforcement, and data loss prevention monitoring.

200.2.6 System & Asset Integrity: Software and firmware shall be designed, implemented, and continuously monitored using integrity protection mechanisms (e.g., integrity verification and monitoring tools, input validation mechanisms, log protection, and secure application design principles). Hardware shall be assessed and monitored using integrity checking mechanisms (e.g., serial number verification, anti-tamper technologies).

200.2.7 Test Data: Development and testing environments shall not utilize production data unless the data has been sanitized or de-identified using DoIT-approved methods that remove or obfuscate non-public information. Use of synthetic data best protects personal information from re-identification or misuse.

200.2.8 Data Privacy: Procedures for the protection of non-public data (Data Classification Level 2 or above) shall be developed in accordance with the minimum standards published by DoIT (i.e., MD-STD-301 through MD-STD-320).

Table 2 RACI Matrix – Data Protection

	DOIT	SCISO/ SCDO/SCPO	Secretaries/ Directors	IT Managers	ISOs
Data at Rest	C	C	A	R	C
Data in Transit	C	C	A	R	C
Data in Use	C	C	A	R	C
Data Availability	C	C	A	R	C
Data Loss Prevention	C	C	A	R	C
System & Asset Integrity	C	C	A	R	C
Test Environments	C	C	A	R	C
Data Privacy	C	C	A	R	C

[R] Responsible, [A] Accountable, [C] Consulted, [I] Informed

200.3 DATA BACKUP & RETENTION

All agencies shall establish data backup and retention requirements in accordance with the following policy:

200.3.1 Backup Requirements: Data owners shall consult with the appropriate data custodians to establish requirements applicable to:

- Backup Frequency: Based on how often critical data changes and how much data loss is acceptable (e.g., Recovery Point Objectives);
- Backup Types: Full, incremental, or differential backups based on time and storage constraints;
- Backup Storage: On-premises, offsite or cloud storage based on availability, security and redundancy goals, and related access restrictions; and
- Backup Testing: Verifying that backup data can be restored successfully and functions as expected in case of data loss or system failure.

200.3.2 Retention Requirements: Data owners shall identify and document in a data retention schedule pursuant to MD Archives, how long each data set should be retained based on the legitimate government purpose for which it was collected, applicable regulatory requirements, and business needs. Personal information should only be retained for as long as it takes to complete the specified purpose for which it was collected, pursuant to its retention schedule, and as defined by applicable regulations and law.

200.3.3 Backup & Retention Agreements: Data owners shall establish, document, and maintain backup and retention agreements with data custodians and perform data backups and retention in accordance with these agreements.

Table 3 RACI Matrix – Data Backup & Retention

	DOIT	SCISO/ SCDO/SCPO	Secretaries/ Directors	IT Managers	ISOs
Backup Requirements	C	C	A	R	C
Retention Requirements	C	C	A	R	C
Backup & Retention Agreements	C	C	A	R	C

[R] Responsible, [A] Accountable, [C] Consulted, [I] Informed

300 APPROVAL

Katie Savage
Secretary & State Chief Information Officer
Maryland Department of Information Technology

James Saunders
State Chief Information Security Officer
Maryland Department of Information Technology

APPENDIX A: POLICY MAPPING MATRIX

This matrix provides a mapping of NIST CSF[1] Best Practices to the sections in this policy for reference.

NIST CSF Category	NIST CSF Sub-Categories	Maryland Policy Mapping
Protect	PR.DS: Data Security	Section 200.3 Data Protection Section 200.4 Data Backup & Retention

[1] NIST Cyber Security Framework 2.0

APPENDIX B: DEFINITIONS

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