DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

Cybersecurity & Privacy Governance 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

100 INTRODUCTION

100.1 PURPOSE

This policy establishes the policy framework through which the State of Maryland defines, implements, and oversees cybersecurity and privacy practices aligned with regulatory requirements, industry standards, and strategic objectives. This policy drives consistency in the management and oversight of the cybersecurity activities distributed across State agencies. The policy suite evolves the State's cybersecurity paradigms from static, network-based perimeter defense to focus more heavily on granular access controls based on users and assets. Protecting the information and information resources entrusted to Maryland from unauthorized access, disclosure, or manipulation is essential to the State's ability to achieve its mission and maintain public trust.

100.2 SCOPE

This policy provides an organizational approach for the governance of all aspects of cybersecurity and is not specific to any single platform or technology solution. This policy addresses all information technology (IT) users, assets and resources that generate, receive, store, process or transmit State data, whether the resources are hosted by the State or hosted by a third-party provider.

100.3 AUTHORIZATION

The Maryland Department of Information Technology (DoIT) is responsible for the development, maintenance, and enforcement of information technology policies, procedures, and standards, and the management, direction, coordination, and implementation of the overall cybersecurity and privacy strategy and policy for units of State government in accordance with State Finance & Procurement Article (SF&P) § 3.5-303, § 3.5-2A-04 and Executive Order 01.01.2021.10. These responsibilities include but are not limited to the establishment of security requirements for information and information systems and the development and maintenance of information technology security and privacy policy, standards, and guidance documents.

100.4 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 simply as "agencies."

100.5 SUPERSEDED POLICY

This policy along with the full policy suite and associated standards outlined in Appendix C supersedes the State of Maryland Information Technology Security Manual Version 1.2, Dated June 28, 2019.

200 POLICY PRINCIPLES

The following principles guide the State's cybersecurity & privacy policy, promoting consistency and alignment with the State's mission, values, and goals.

- **Provide Value for State of Maryland Objectives:**
  Establish security policies that enable the shared mission of the State Chief Information Security Officer (SCISO), the State Chief Privacy Officer (SCPO) and the State Chief Data Officer (SCDO), to protect the confidentiality, integrity and availability of State data and information assets, by assisting agencies in timely decision-making, flexible response to organizational changes, and meeting evolving business needs with IT solutions that are secure and compliant with State's legal, regulatory, and executive order requirements.
- **Shift to Zero Trust Model**
  Shift the State away from the traditional "trust but verify" approach to a "never trust, always verify" mindset, particularly for High Value State Systems (HVSS), by requiring continuous validation of identities and security postures. ZTA is based on the principle that no device, user, or asset should be trusted solely based on its location within a network. The framework requires all users, whether inside or outside the organization's network, to be continuously authenticated, authorized, and validated before being granted access to applications and data.
- **Establish Institutional Cybersecurity Risk Profile**
  Identify, assess, and maintain an acceptable operational risk level across all agencies and support the transfer of cybersecurity risk to individual agency Authorizing Officials (AO) for acceptance in alignment with their cybersecurity risk tolerance.
- **Provide Clear, Unambiguous Direction**
  Establish a comprehensive cybersecurity and privacy policy governance structure that applies uniformly across all agencies, clearly defining roles, responsibilities, and expectations.

- **Establish Distinct Cybersecurity Roles**
  Establish the set of required cybersecurity roles that are commonly distributed among each agency and their associated responsibilities in executing cybersecurity and privacy policy.
- **Align with State's Cybersecurity & Privacy Policies**
  Promote alignment among each agency to the State's cybersecurity and privacy policies through consistent application of cybersecurity and privacy standards. Privacy standards will align with Federal privacy practices. Cybersecurity policies will be driven by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) categories: a) *Govern*, b) *Identify*, c) *Protect*, d) *Detect*, e) *Respond*, and f) *Recover.*

300 RESPONSIBILITY

300.1 DEPARTMENT OF INFORMATION TECHNOLOGY

The DoIT Office of Security Management (OSM) is responsible for developing cybersecurity and privacy policy and standards for consistency across all agencies. OSM responsibilities as they relate to this policy include, but are not limited to:

- Delivering cybersecurity and privacy leadership through the SCISO and SCPO to develop and implement the State's cybersecurity and privacy program and proactively manage risk;
- Reviewing and updating cybersecurity and privacy policy and standards at least annually in accordance with changes in technology, organizational responsibility, and changes across the threat landscape;
- Implementing an Enterprise Risk Management (ERM) strategy, including an Authorization to Operate (ATO) Process;
- Implementing shared Enterprise Architecture (EA) standards for consistency, interoperability, and alignment with the State's strategic goals promoting ZTA principles that require all users, whether inside or outside the organization's network, to be continuously authenticated, authorized, and validated before being granted access to applications and data;
- Coordinating response activities across the agencies, other applicable State government entities, and external resources (e.g., CISA) as needed to minimize damages to State information resources; and
- Coordinating with the SCISO and SCPO for any policy exception requests following the OSM waiver process.

300.2 EXECUTIVE BRANCH SECRETARIES, EXECUTIVE DIRECTORS, AND ADMINISTRATORS

The Secretaries, Directors, and Administrators (or equivalents) who oversee different departments and agencies are responsible for managing their respective agencies' compliance with the State cybersecurity and privacy policies and standards. Secretaries, Directors, and Administrators' responsibilities include, but are not limited to:

- Making all personnel within the agency aware of and compliant with State cybersecurity and privacy policy and standards published by DoIT and applicable regulatory requirements;
- Aligning all IT acquired by the agency with cybersecurity and privacy policy and standards, and applicable regulatory requirements;
- Maintaining oversight and responsibility for the security of IT assets and data flow within their area of control;
- Implementing and maintaining an agency cybersecurity and privacy program that aligns to and implements State cybersecurity and privacy policy, standards, and regulatory compliance;
- Accurately classifying its data based upon the State Data Classification Policy in order to determine the degree of data protection required;
- Implement any applicable regulatory requirements as part of agency-level procedures;
- Performing annual self-assessments to validate the effectiveness of the agency cybersecurity and privacy program (and/or provide support to DoIT-led assessments as requested);
- Abiding by the agency-defined retention guidelines approved by the Maryland State Archives;
- Collaborating with the SCISO (or designee) when solicited for input during annual policy and standard updates; and
- Coordinating with the SCISO and SCPO for any policy exception requests following the OSM waiver process.

300.3 INFORMATION SECURITY OFFICERS

The Information Security Officer (ISO) program is a shared service provided by DoIT to support State agencies in strengthening their cybersecurity posture and driving adoption of State Cybersecurity Shared Services (i.e., DoIT-managed services) where efficiencies may be gained. The ISOs provide security expertise, guidance, and resources to assist agencies in meeting State and Federal cybersecurity requirements. The service provides agencies with

access to experienced cybersecurity professionals who can assist with managing risk, implementing security controls, and coordinating incident response efforts. The ISO responsibilities include, but are not limited to:

- Providing cybersecurity expertise and support to assigned agency or agencies;
- Working with agencies to complete the Maryland State ATO Process, which includes assisting with documentation, collaborating with stakeholders, obtaining signatures, and selecting additional controls;
- Serving as security control assessors as part of the Maryland State ATO Process (as needed);
- Making recommendations for risk remediation;
- Guiding agency personnel in developing agency-level procedures aligned with State cybersecurity and privacy policy and standards;
- Assisting agency personnel with understanding, and interpretation of the State's ZTA principles of: a) never trust, always verify; b) least privilege access, c) assume breach, d) continuous monitoring and validation, e) strong authentication and authorization, f) micro segmentation, and g) policy-based access control;
- Helping identify technology and human resource needs related to meeting policy and standards;
- Providing compliance support for State and Federal regulations;
- Promoting State-wide and agency-specific security awareness training and education programs;
- Providing incident response coordination and reporting;
- Providing recommendations for vendor risk management activities;
- Assisting agency personnel in the evaluation of policy exception requests following the OSM waiver process; and
- Delivering security consultation and advisory services.

300.4 INFORMATION TECHNOLOGY MANAGERS

Any staff with the responsibility of procuring and operating IT for their respective agencies are responsible for:

- Protecting State data within their purview by applying adequate controls based on the data's protection needs in accordance with the MD-POL-205 Data Protection & Privacy Policy and applicable regulatory drivers;
- Documenting and maintaining System Security Plans (SSP) for each system within their purview;

- Evaluating all IT for risk prior to procurement (or being placed into production) and verifying that security policy is implemented throughout the system's lifecycle; and
- Complying with all emergency directives and binding operational directives immediately upon issuance (or report anticipated delay in completion directly to OSM).

300.5 INFORMATION USERS

Individual users of State data and IT assets, whether employees, contractors, volunteers or temporary workers, are responsible for protecting State data and assigned IT assets. User's responsibilities include, but are not limited to:

- Reviewing, complying with, and maintaining awareness of applicable State-published cybersecurity and privacy policy and standards (e.g., MD-POL-203 Acceptable Use Policy);
- Reviewing, complying with, and maintaining awareness of procedures and guidelines that are specific to their agency;
- Reporting cybersecurity and privacy incidents in alignment with the State incident response policy (e.g., MD-POL-209 Incident Response Policy); and
- Reporting any observed or suspected non-compliance with applicable State cybersecurity and privacy in alignment with policy and standards, or agency procedures and guidelines to their direct manager.

400 POLICY

The following sections detail the State's Cybersecurity and Privacy Policy Suite which is comprised of a portfolio of policies, directives, and standards.

400.1 POLICY HIERARCHY

The multi-tier hierarchy is organized as follows:

400.1.1 State of Maryland Cybersecurity Governance Policy (100-Level): This policy supports the cybersecurity and privacy governance across the Executive Branch. This policy transcends all agencies and deals with general cybersecurity and privacy subject areas and serves as a foundation for topic-specific functional policies.

DoIT may issue directives at any time to protect State information systems and data from imminent threats and emerging technologies as follows:

- Emergency Directives (ED): A mandatory instruction requiring specific actions to address a significant cybersecurity threat, vulnerability, or incident. These directives typically address a specific product, technology or avenue of exploit; and are issued in

response to an immediate or urgent situation that requires prompt action to protect the State, its assets, or its personnel. Usually short-term and in effect only for the duration of the emergency.

- Binding Operational Directive (BOD): A mandatory instruction requiring specific actions to safeguard Maryland information systems. Each directive is applicable to the State units, or other State-owned network users, identified in the directive. These directives typically address internal cybersecurity practices required to mitigate operational risk; are issued to establish and maintain uniform practices in a specific area of risk; and are generally long-term and remain in effect until officially modified or revoked.

400.1.2 State of Maryland Cybersecurity Functional Policies (200-Level): These policies address specific cybersecurity domains or sub-mission areas of current relevance to the State. This policy set aligns to the NIST CSF categories and subcategories and supports the creation of standards specific to operational cybersecurity subjects.[1]

400.1.3 State of Maryland Cybersecurity Standards (300-Level): Standards address the requirements agencies must implement to achieve compliance with the higher-level policies. Standards align to the NIST Special Publication 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations with Organizationally Defined Parameters (ODPs) defined by DoIT OSM. All standards map back to functional policies for enforcement in alignment with the NIST-published mapping between the NIST Cybersecurity Framework (CSF) and NIST SP 800-53[2] to ensure consistent control interpretation, traceability, and functional alignment across the State's cybersecurity program.

400.1.4 Agency-Level Procedures (400-Level): The SCISO recommends agencies establish lower-level procedures and guidelines aligned to State policy standards. The SCISO will provide templates to assist agencies in the development of lower-level standard operating procedures along with specific implementation-level guidance where further enhancement of the State's security posture is prudent.

[1] National Institute of Standards and Technology Cybersecurity Framework Version 2.0

[2] CSF 2.0 Informative References | NIST

State agencies retain the discretion to tailor their agency-level policies, procedures and guidelines to reflect their unique organizational processes as long as they do not contradict State policy. However, any such policies and procedures must incorporate the State of Maryland Cybersecurity Standards (300-Level) as a minimum baseline. Agencies may adopt more restrictive or prescriptive measures but should not implement standards that are less rigorous than those set forth in the standards.

400.2 POLICY ADMINISTRATION

DoIT will administer the cybersecurity policy portfolio as follows:

400.2.1 Responsibility: The SCISO and the SCPO are responsible for State's cybersecurity and privacy policy administration and may delegate responsibility for policy maintenance and implementation as appropriate within DoIT.

400.2.2 Coordination: The SCISO or the assigned delegate will coordinate cybersecurity and privacy policy activities with the other agencies for feedback prior to publishing.

400.2.3 Maintenance: The SCISO or the assigned delegate will establish and implement lifecycle management activities to regularly maintain cybersecurity policy, standards, and supporting documentation.

400.2.4 Enforcement: The SCISO or the assigned delegate will review and validate that agencies adhere to the State's cybersecurity and privacy policies and standards.

400.2.5 DoIT-Managed Services: When an agency consumes a DoIT-managed service, such as statewide network security, identity services, or centrally managed platforms, the controls implemented and maintained by DoIT apply directly to the agency's environment, eliminating the need for redundant effort and ensuring consistent, statewide adherence to policy. Because DoIT-managed services differ in scope, architecture, and adoption across agencies, the statewide policy suite cannot prescribe specific requirements for those services or define their control implementations. Instead, when an agency chooses to consume a DoIT-managed capability the controls built and maintained by DoIT apply directly to that agency's environment. This inherited compliance model eliminates redundant effort, promotes consistency where shared services are used, and strengthens the statewide security posture, while still requiring agencies to implement any controls not covered by the enterprise service or for which they maintain local responsibility.

400.3 WAIVERS

Agencies may submit exception requests and receive waivers to State cybersecurity and privacy policy and standards as follows:

400.3.1 Waivers: Agencies may request an exception via the waiver process when technical or operational constraints make it infeasible to comply with a policy requirement or standard. All waiver requests must originate at the agency level and follow the OSM-approved waiver process. The Agency AO may approve waivers when compliance is prevented by such constraints, and the request provides a compelling justification such as an unusual circumstance or an unintended hardship created by the policy or standard. Waivers involving HVSS must be escalated to and approved by the State CISO. All approved waivers must be time-bound, not to exceed 12 months, and document the mitigating or compensating controls that will be implemented to reduce risk to an acceptable level for the duration of the waiver.

400.3.2 Risk-Based Decision Making: In alignment with the MD-POL-201 Cybersecurity Risk Management Policy, the Agency AO and the SCISO will consider planned and applied risk mitigations when making waiver decisions.

400.4 FUNCTIONAL AREA POLICIES

The SCISO will establish policy and supporting standards that address each functional area defined by the NIST Cybersecurity Framework 2.0 as follows:

400.4.1 MD-POL-201 Cybersecurity Risk Management: A cybersecurity risk management strategy, expectations, and policy shall be established, communicated, and monitored to include the management of third-party risk.

400.4.2 MD-POL-202 Asset Management: Assets (e.g., data, hardware, software, systems, facilities, services, people) shall be identified and managed consistent with their relative importance to State objectives and strategy.

400.4.3 MD-POL-203 Acceptable Use Policy: The acceptable use of State-owned or managed assets shall be documented, approved, and communicated to all IT users.

400.4.4 MD-POL-204 Access Control: Access control policy shall be established to address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with applicable laws, executive orders, directives, and regulations.

400.4.5 MD-POL-205 Data Protection & Privacy: State data shall be managed in alignment with the State's risk strategy to protect the confidentiality, integrity, and availability of information as well as promote its accuracy, currency, and completeness.

400.4.6 MD-POL-206 Security Awareness & Privacy Training: All personnel and partners shall be provided cybersecurity and privacy awareness education and trained to perform their cybersecurity and privacy-related duties and responsibilities consistent with related policies, procedures, and agreements.

400.4.7 MD-POL-207 System & Network Security: Security architectures, hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms shall be managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and contributes to organizational resilience.

400.4.8 MD-POL-208 Continuous Monitoring: A continuous monitoring program shall facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.

400.4.9 MD-POL-209 Incident Response: An incident response capability shall be developed and maintained to react and contain the impact of a potential cybersecurity incident.

400.4.10 MD-POL-210 Continuity of Operations: Restoration activities shall be coordinated with internal and external parties in a manner that support continuity of essential mission and business functions during and after a cybersecurity or privacy incident.

400.5 REGULATORY COMPLIANCE

Each agency is responsible for accurately classifying its data in accordance with the State Data Classification Policy to determine the appropriate level of protection. When specific data types are governed by state laws or regulatory requirements, agencies must integrate those obligations into their internal procedures and operational practices. If any applicable State law, Executive Order, or regulatory requirement imposes stricter protections or creates a conflicting obligation that prevents adherence to State cybersecurity policies or standards, the legal or regulatory requirement takes precedence

500 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[3] Best Practices to the sections in this policy for reference.

NIST CSF Category	NIST CSF Sub-Categories	Document Mapping
Govern	GV.OC Organizational Context	100 Introduction
Govern	GV.RM Risk Management	200 Policy Principles
Govern	GV.RR: Roles, Responsibilities, and Authorities	300 Responsibility; 400.4.3 Acceptable Use Policy
Govern	GV.PO: Policy	400 Policy
Govern	GV.OV: Oversight	400.2 Policy Administration
Govern	GV.SC: Cybersecurity Supply Chain & Risk Management	400.4.1 CS Risk Management
Identify	ID.AM: Asset Management	400.4.2 Asset Management
Identify	ID.RA: Risk Assessment	400.4.1 CS Risk Management
Identify	ID.IM: Improvement	400.4.1 CS Risk Management
Protect	PR.AA: Identity Management, Authentication, and Access Control	400.4.4 Access Control
Protect	PR.AT: Awareness and Training	400.4.5 Awareness & Training
Protect	PR.DS: Data Security	400.4.6 Data Protection & Privacy
Protect	PR.PS: Platform Security	400.4.7 System & Network Security
Protect	PR.IR: Technical Infrastructure Resilience	400.4.7 System & Network Security
Detect	DE.CM: Continuous Monitoring	400.4.8 Continuous monitoring
Detect	DE.AE: Adverse Event Analysis	400.4.8 Continuous monitoring
Respond	RS.MA: Incident Management	400.4.9 Incident Response
Respond	RS.AN: Incident Analysis	400.4.9 Incident Response
Respond	RS.CO: Incident Response Reporting and Communication	400.4.9 Incident Response
Respond	RS.MI: Incident Mitigation	400.4.9 Incident Response
Recover	RC.RP: Incident Recovery Plan Execution	400.4.10 Continuity of Operations
Recover	RC.CO: Incident Recovery Communication	400.4.10 Continuity of Operations

[3] NIST Cybersecurity Framework 2.0

APPENDIX B: DEFINITIONS

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

APPENDIX C: RELATED POLICY DOCUMENTS

This policy is part of broader Maryland Cybersecurity and Privacy Policy Suite designed to address the full spectrum of cybersecurity domains. The full suite of policies and standards are listed below.

100-Series

The governance policy establishes the policy framework through which the State of Maryland defines, implements, and oversees cybersecurity and privacy practices.

Doc ID	Title/Subject
MD-POL-100	Cybersecurity & Privacy Governance Policy

200-Series

The functional policies address organizational commitment to the specific cybersecurity domains driven by NIST Cyber security Framework.

Doc ID	Title/Subject
MD-POL-201	Cybersecurity Risk Management Policy
MD-POL-202	Asset Management Policy
MD-POL-203	Acceptable Use Policy
MD-POL-204	Access Control Policy
MD-POL-205	Data Protection & Privacy Policy
MD-POL-206	Awareness & Training Policy
MD-POL-207	System and Network Security Policy
MD-POL-208	Continuous Monitoring Policy
MD-POL-209	Incident Response Policy
MD-POL-210	Continuity of Operations Policy

300- Series

The standards define requirements agencies must implement to achieve compliance with the higher-level policies driven by NIST 800-53 Rev 5.

Doc ID	Title/Subject
MD-STD-301-AC	Access Control Standard
MD-STD-302-AT	Awareness & Training Standard
MD-STD-303-AU	Audit & Accountability Standard
MD-STD-304-CA	Control Assessments Standard
MD-STD-305-CM	Configuration Management Standard
MD-STD-306-CP	Contingency Planning Standard

Doc ID	Title/Subject
MD-STD-307-IA	Identification & Authentication Standard
MD-STD-308-IR	Incident Response Standard
MD-STD-309-MA	Maintenance Standard
MD-STD-310-MP	Media Protection Standard
MD-STD-311-PE	Physical & Environmental Protection Standard
MD-STD-312-PL	Planning Standard
MD-STD-313-PM	Program Management Standard
MD-STD-314-PS	Personnel Security Standard
MD-STD-315-PT	PII and Transparency Standard
MD-STD-316-RA	Risk Assessment Standard
MD-STD-317-SA	System & Services Acquisition Standard
MD-STD-318-SC	System & Communication Protection Standard
MD-STD-319-SI	System & Information Integrity Standard
MD-STD-320-SR	Supply Chain & Risk Management Standard