DEPARTMENT OF INFORMATION TECHNOLOGY
Office of Security Management

Cybersecurity Risk Management 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

CYBERSECURITY RISK MANAGEMENT POLICY

MD-POL-201-01	Last Updated: 02/18/2026

100 INTRODUCTION

Purpose:	This policy establishes the requirements for managing information security risk to the State by assessing risk, responding to risk once determined, and monitoring risk over time.
Scope:	This policy provides an organizational approach for risk management that addresses all information technology (IT) assets that generate, receive, store, process, or transmit State data, whether the system 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Superseded Policy:	The full policy suite outlined in MD-POL-100 Cybersecurity & Governance Policy, Appendix C supersedes the State of Maryland Information Technology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.
	Data Owners (DO): An individual or group responsible for a specific data asset or group of data assets within an Agency.

	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 of 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 and privacy compliance requirements.
	Information User (hereafter referred to simply as "user") - Any person who interacts with a State computer system, software application, network service, or data to include State employees, contractors, vendors, third-party providers.
Risk Management Roles:	The NIST Risk Management Framework introduces specific risk management roles as follows: **Authorizing Official (AO)** - A senior official or executive with the authority to formally assume responsibility for operating an

	information system at an acceptable level of risk to organizational operations, organizational assets, and individuals. **System Owner (SO)** - A person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system. Note: The System Owner may also serve as the AO.
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 cybersecurity risk management policy which aligns to the Zero Trust Architecture (ZTA) principles by shifting the security paradigm from implicit trust to continuous verification.

200.1 RISK APPETITE & TOLERANCE

200.1.1 Organizational Risk: The SCISO oversees the State's Enterprise Risk Management Strategies and related programs which will guide agency Authorizing Officials (AO) in establishing a risk appetite for their respective agencies.

200.1.2 System-Level Risk Tolerance: Agency IT managers shall be responsible for managing each system under their purview within the risk tolerance defined by the appropriate agency AO based on the information contained within and their capacity to manage, mitigate, and recover from potential adverse events.

200.1.3 Risk Oversight: The SCISO shall maintain oversight of the organizational cybersecurity risk posture, providing risk mitigation recommendations to agencies, promoting agency use of risk registries for known and accepted risks, and update State policies and standards as needed to continuously improve the State's risk posture.

200.1.4 Risk Assessments: Agencies shall utilize and follow the SCISO and SCPO-approved methodology for assessing, documenting, categorizing, and prioritizing cybersecurity and privacy risks.

200.1.5 Data Classification: Data Owners within each agency shall be responsible and accountable for classifying and handling State data, under their purview, based on the risk level to stakeholders as defined by the Data Classification Policy and as directed by the Office of Enterprise Data (OED), State Chief Data Officer (SCDO), Agency Data Officers (ADO), and State data governance policy and guidelines.

Table 1 RACI Matrix – Risk Appetite & Tolerance

	DOIT	SCISO/ DOs	Secretaries/ Directors	IT Managers	ISOs
Organizational Risk Appetite	-	R, A	I	I	-
System-level Risk Tolerance	-	C	R, A	I	C
Risk Oversight	R	A	C	I	C
Risk Assessments	C	R, A	I	I	C
Data Classification	-	I	A	R	C

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

200.2 ENTERPRISE RISK MANAGEMENT STRATEGY

Agencies are responsible for adhering to the SCISO and SCPO-approved comprehensive strategy for managing the risk across their IT systems, including but not limited to completing the State Authorization to Operate (ATO) Process. The ISOs shall work with agencies to complete the ATO process procedures, including assistance with documentation, stakeholder coordination, signature collection, and control selection. As deemed appropriate by the SCISO, the MD State ATO process may incorporate the following risk management activities:

200.2.1 Prepare: Determine the risk management roles, responsibilities, risk tolerance, risk assessment and authorization methods to be used with each agency.

200.2.2 Categorize: Perform an impact analysis for each system that identifies the information types to be processed and the security protection requirements to be implemented, considering the classification of all data within the system.

200.2.3 Select: Choose the appropriate security controls, best practices, and State standards that will protect the system, and its information based on the outcome of categorization.

200.2.4 Implement: Implement security controls, best practices, and State standards prior to placing a system into production, and maintain a Plan of Action and Milestones (POA&M) for any planned security controls or flaw remediation. Implementation of security controls shall enforce ZTA principles through strict access controls, continuous authentication, and least privilege principles.

200.2.5 Assess: Evaluate applied security controls prior to placing a system into production to verify that they are implemented correctly and functioning as intended.

200.2.6 Authorize: Obtain a formal, risk-based decision by the appropriate AO to either authorize or deny system operation at the assessed risk level.

200.2.7 Monitor: Establish and implement an information security continuous monitoring program that regularly monitors all operational systems for ongoing risk.

Table 2 RACI Matrix – Enterprise Risk Management Strategy

	DOIT	SCISO/ DOs	Secretaries/ Directors	IT Managers	ISOs
Prepare	C	C	R, A	I	C
Categorize	C	I	A	R	C
Select	C	I	A	R	C
Implement	C	I	A	R	C
Assess	C	I	A	R	C
Authorize	C	I	A	R	C
Monitor	C	I	A	R	C

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

200.3 RISK ASSESSMENTS

To understand and respond to the risk associated with any State system housing or processing State data, agencies shall perform each of the following assessments for systems within their purview:

200.3.1 Security Vulnerability Assessments: Deploy vulnerability management practices and technologies to identify vulnerabilities across all facilities, assets, networks, and software.

200.3.2 Privacy Impact Assessments: Perform Privacy Threshold Analysis (PTA) and if required Privacy Impact Assessments (PIA) as directed by the SCPO.

200.3.3 Network & Architecture Assessments: Assess network and architecture designs to identify weaknesses that affect a system's cybersecurity and configuration management. Assessments shall include review of network segmentation and access policy enforcement to align to ZTA and reduce the potential entry points for attackers.

200.3.4 Software Security Assessments: Identify design, software code, and default configuration vulnerabilities for all State-developed software.

200.3.5 Physical Security Assessments: Coordinate with facilities personnel as needed to assess the physical protection of critical computing assets.

200.3.6 Threat Intelligence Assessments: Monitor sources of cyber threat intelligence for information on new vulnerabilities associated with any products and services operated within the Agency.

200.3.7 Process & Procedural Assessments: Review IT and security processes and procedures for weaknesses that could be exploited (e.g., change management).

200.3.8 Vulnerability Disclosure Program: All Maryland-affiliated properties, systems, and digital assets are subject to the state's Vulnerability Disclosure Program (VDP). This includes websites, applications, APIs, and infrastructure components managed by or on behalf of state agencies. Agencies will be required to remediate vulnerabilities exposed by this program as directed by DoIT OSM.

Table 3 RACI Matrix – Risk Assessments

	DOIT	SCISO/ SCPO	Secretaries/ Directors	IT Managers	ISOs
Security Vulnerability Assessments	I	C	A	R	C
Privacy Impact Assessments	I	C	-	-	R*
Network & Architecture Assessments	I	C	A	R	C
Software Security Assessments	I	C	A	R	C
Physical Security Assessments	I	C	A	R	C
Threat Intelligence Assessments	I	C	A	R	C
Process & Procedural Assessments	I	C	A	R	C
Vulnerability Disclosure Program	R	A	I	C	C

**ISOs shall coordinate with the Agency Privacy Officers (APOs) and Agency Data Officers (ADOs) where such roles exist within an agency.*

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

200.4 THIRD PARTY RISK MANAGEMENT

The SCISO is responsible for maintaining policy and standards for third party risk management. All agencies shall extend State cybersecurity policies and standards to suppliers, customers, and partners as follows:

200.4.1 Supplier Criticality: Identify IT product and service suppliers by business criticality (e.g., operational dependency, security impact, available alternatives).

200.4.2 Supplier Risk Management: Apply each activity outlined in Section 200.2 to the supply chain so that external vendors or third-party suppliers are not blindly trusted.

200.4.3 Supplier Assessments: Establish methods to assess supplier risk in coordination with DoIT and the Department of General Services (DGS) Office of State Procurement (e.g., procurement process improvements where appropriate).

200.4.4 Contract Language: Incorporate security and privacy control requirements into contracts and other types of agreements with suppliers and other relevant third parties in alignment with SCISO guidance.

200.4.5 Supplier Due Diligence: Perform cybersecurity risk management planning and due diligence to reduce risks before entering into formal supplier or other third-party relationships.

200.4.6 Supplier Monitoring: Continuously monitor suppliers or other third parties over the life of the relationships.

200.4.7 Contract Termination: Upon the conclusion of any IT partnership, contract, or service agreement, the agency shall implement and enforce cybersecurity measures such as data removal and access revocation to safeguard information assets and maintain compliance with applicable regulations.

Table 4 RACI Matrix – Third Party Risk Management

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Supplier Criticality	C	I	A	R	C
Supplier Risk Management	C	I	A	R	C
Supplier Assessments	C	I	A	R	C
Contract Language	C	I	A	R	C
Supplier Due Diligence	C	I	A	R	C
Supplier Monitoring	C	I	A	R	C
Contract Termination	C	I	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
Govern	GV.RM: Risk Management Strategy	Section 200.2 Enterprise Risk Management Strategy
Govern	GV.OV: Oversight	Section 200.1.3 Risk Oversight
Govern	GV.SC: Cybersecurity Supply Chain Risk Management	Section 200.4 Third Party Risk Management
Identify	ID.RA: Risk Assessment	Section 200.3 Risk Assessments
Identify	ID.IM: Improvement	Section 200.1.3 Risk Oversight

[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**.