DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

Awareness & Training 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.

State of Maryland

AWARENESS & TRAINING POLICY

MD-POL-206-01	Last Updated: 02/18/2026

TABLE OF CONTENTS

CHANGE RECORD

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

State of Maryland

AWARENESS & TRAINING POLICY

MD-POL-206-01	Last Updated: 02/18/2026

100 INTRODUCTION

Purpose:	This policy establishes the requirements for developing and maintaining an awareness and training program for cybersecurity and privacy.
Scope:	This policy addresses awareness and training for all State information users with additional role-based training for staff performing specialized tasks with elevated permissions.
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Superseded Policy:	The full policy suite outlined in MD-POL-100 Cybersecurity & Governance Policy, Appendix C supersedes the State of Maryland Information Technology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.

	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 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.
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 cybersecurity and privacy awareness and training activities required to reduce human risk, ensure regulatory compliance, and build a culture of security and privacy protection across the State.

200.1 CYBERSECURITY & PRIVACY AWARENESS

200.1.1 General Awareness: The DoIT Office of Security Management (OSM), in collaboration with the Office of Enterprise Data (OED), will design and deliver cybersecurity and privacy awareness materials that equip State information users to perform their duties with cybersecurity, privacy, and data-management risks in mind. This training will reinforce common cybersecurity and privacy principles by emphasizing the importance of access controls and recognizing potential threats. OSM will maintain completion records for all personnel who complete the required cyber awareness training.

Agencies are highly encouraged to take advantage of the standardized cyber training program delivered by OSM, which ensures consistency, accountability, and enterprise-wide alignment. For agencies that currently operate their own training programs, OSM will require submission of training materials and completion records to support State-wide monitoring and compliance.

Table 1 RACI Matrix – Cybersecurity & Privacy Awareness

	DOIT	SCISO/ SCPO	Secretaries/ Directors	IT Managers	ISOs
General Awareness	R	A	I	I	C

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

200.2 CYBERSECURITY TRAINING

200.2.1 Role-Based Cybersecurity Training: In addition to the enterprise awareness training OSM will provide role-based training for individuals with cybersecurity-related job duties (e.g., privileged access and implementation of cyber tools) to build the knowledge, skills, and abilities required to effectively perform assigned tasks. Individuals performing a cybersecurity role shall be trained in the cybersecurity responsibilities of that role (e.g., enforcing access controls and monitoring security events). Role-based training will be

periodically updated as threats and technologies change. Training may be extended to individuals in other departments such as Finance and Human Resources as deemed appropriate by the SCISO based on their access to non-public data (Data Classification Level 2 or above).

Table 2 RACI Matrix – Cybersecurity Training

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Role-Based Training	C	C	A	R	C

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

200.3 PRIVACY TRAINING

200.3.1 Role-Based Privacy Training: In addition to the enterprise awareness training provided by OSM, all agencies shall provide role-based training to individuals with privacy-related job duties to build the knowledge, skills and abilities required to effectively perform assigned tasks. Agencies shall maintain completion records for all personnel who complete the required privacy training. Training shall be regularly updated based on incidents, audits, privacy-by-design principles and best practices, or changes in privacy laws and policies. Training may be extended to individuals in other departments such as Finance and Human Resources based on their access to information defined by the State as either confidential or restricted (Data Classification Level 3 or 4). Agency IT managers may consult Agency Privacy Officer and DoIT to determine appropriate role-based training curriculum.

Table 3 RACI Matrix – Privacy Training

	DOIT	SCPO	Secretaries/ Directors	IT Managers	ISOs
Role-Based Training	C	C	A	R	C

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

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.AT: Awareness & Training	Section 200.1

[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**.