DEPARTMENT OF INFORMATION TECHNOLOGY
Office of Security Management

Information Security Continuous Monitoring 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

100 INTRODUCTION 2
200 POLICY 4
200.1 NETWORK & SYSTEM MONITORING 4
200.2 PHYSICAL ENVIRONMENT MONITORING 5
200.3 PERSONNEL MONITORING 5
200.4 EXTERNAL SERVICE PROVIDER MONITORING 6
200.5 EVENT ANALYSIS 6
300 APPROVAL 6
APPENDIX A: POLICY MAPPING MATRIX 7
APPENDIX B: DEFINITIONS 8

CHANGE RECORD

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

100 INTRODUCTION

Purpose:	This policy establishes the requirements for maintaining ongoing awareness of information security risks, vulnerabilities, and threats to enable timely and effective threat response within the State of Maryland.
Scope:	This policy addresses the monitoring of all State systems whether operated by the State 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Superseded Policy:	The full policy suite outlined in MD-POL-100 Cybersecurity & Governance Policy, Appendix C supersedes the State of Maryland Information Technology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.

	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 monitoring required to implement Zero Trust Architecture (ZTA) principles that provide real-time visibility, detection of anomalies, and enforcement of dynamic security policies.

200.1 NETWORK & SYSTEM MONITORING

200.1.1 Monitoring Strategy: All agencies shall develop and implement a system-level continuous monitoring strategy in accordance with the State standards published by DoIT. All monitoring strategies shall be designed with the following ZTA goals:

- Real-Time Threat Detection;
- Identity Verification & Authentication;
- Least Privilege Enforcement;
- Micro-segmentation Analytics; and
- Automated Response Mechanisms.

All operating systems, applications, and services including subscription-based services must be configured to generate appropriate log records. These logs shall be transmitted to agency authorized audit-reduction tools and to the DOIT Office of Security Management (OSM) centralized audit record management solution.

200.1.2 Network Monitoring: All on-premises environments, IT networks, and cloud platforms shall be continuously monitored to identify anomalous or otherwise adverse user behavior and network activity, with comprehensive logging, automated alerting, and full integration into incident detection and response processes.

200.1.3 System Monitoring: All State systems shall be configured to monitor for:

- Authentication attempts to identify attacks against credentials and unauthorized credential reuse;
- Ongoing verification of identities (not just one-time authentication);
- Software configurations for deviations from security baselines;
- Cyber health issues (e.g., missing patches, malware infections, unauthorized software);
- Hardware and software for signs of tampering;
- Malicious code at system entry and exit points;
- Unauthorized mobile code;
- Unauthorized personnel, connections, devices, and software; and
- Vulnerabilities in the system and hosted applications.

Table 1 RACI Matrix – Network & System Monitoring

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Monitoring Strategy	C	I	A	R	C
Network Monitoring	C	I	A	R	C
System Monitoring	C	I	A	R	C

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

200.2 PHYSICAL ENVIRONMENT MONITORING

200.2.1 Physical Environment: The physical environments housing State systems (e.g., server rooms, network closets, patch panels) shall be monitored to detect potentially adverse events (e.g., badge readers, physical access records, access control tampering).

Table 2 RACI Matrix – Physical Environment

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Physical Environment	C	I	A	R	C

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

200.3 PERSONNEL MONITORING

200.3.1 Personnel Monitoring: Personnel activity and technology usage will be monitored solely for the purpose of detecting potentially adverse events and ensuring the security and integrity of State systems. This monitoring relies on existing tools such as user-behavior analytics, log monitoring, detection technologies, and manual log reviews. These activities do not include employee surveillance, productivity tracking, recording of screens, or keystrokes, or audio/video.

Table 3 RACI Matrix – Personnel Monitoring

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Personnel Monitoring	C	I	A	R	C

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

200.4 External Service Provider Monitoring

200.4.1 External Service Providers: External service providers shall be monitored to detect potentially adverse events (e.g., remote access monitoring, service providers anomalies).

Table 4 RACI Matrix – External Service Providers

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
External Service Providers	C	I	A	R	C

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

200.5 Event Analysis

200.5.1 Adverse Events: Potentially adverse events shall be analyzed to:

- Better understand targets and methods;
- Correlate information from multiple monitoring sources;
- Estimate impact and scope;
- Generate alerts and distribute to authorized staff and tools; and
- Gain contextual information through cyber threat intelligence.

200.5.2 Incident Declaration: Incident criteria shall be applied to known and assumed characteristics of activity in order to determine whether an incident should be declared in accordance with the MD-STD-308-IR Incident Response Standard.

Table 5 RACI Matrix – Event Analysis

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Adverse Events	C	I	A	R	C
Incident Declaration	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 Document
Detect	DE.CM: Continuous Monitoring	Section 200.1, 200.2, 200.3, 200.4
Detect	DE.AE: Adverse Event Analysis	Section 200.5

[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**.