DEPARTMENT OF
INFORMATION TECHNOLOGY
Office of Security Management

System & Network Security 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

SYSTEM & NETWORK POLICY

MD-POL-207-01 **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

SYSTEM & NETWORK POLICY

MD-POL-207-01 | **Last Updated: 02/18/2026**

100 INTRODUCTION

Purpose:	This policy establishes the requirements for managing the hardware, software, and services of physical and virtual platforms to protect their confidentiality, integrity, and availability.
Scope:	This policy addresses all State hardware, software (e.g., firmware, operating systems, applications) and services of physical and virtual platforms (e.g., security architectures) 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Superseded Policy:	The full policy suite outlined in MD-POL-100 Cybersecurity & Governance Policy, Appendix C supersedes the State of Maryland Information Technology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 promote foundational system and network security activities required to implement principles of a Zero Trust Architecture (ZTA).

200.1 PLATFORM SECURITY

200.1.1 Configuration Management: All configurable IT assets shall be deployed and maintained in alignment with an established security configuration baseline commensurate with risk, exposure, industry best practices (i.e. Center for Information Security (CIS) benchmarks and vendor recommendations).

200.1.2 Software Security: All IT software shall be managed and protected from vulnerabilities in alignment with an established vulnerability management plan that includes at a minimum:

- Software Patching: Apply security updates according to established timelines;
- Lifecycle Management: Replace or remove unsupported (end-of-life (EOL) and end-of-service (EOS)) software that no longer receives security updates;
- Attack Surface Reduction: Remove unnecessary software following the principle of least functionality, retaining only software with documented business justification; and
- Virtual Environment Management: Keep container and virtual machine images updated with current security patches.

200.1.3 Hardware Security: In alignment with the MD-POL-202 Asset Management Policy, all IT equipment shall be maintained, replaced, and removed in accordance with the following:

- Replacement when hardware no longer supports software security capabilities (i.e., end-of-life);
- Secure disposal; and
- Media sanitization.

200.1.4 Audit Logs: 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. Agencies shall protect all log data from unauthorized access and maintain it for a defined retention period. The retention period must be established by each agency based on its risk tolerance and applicable regulatory requirements.

200.1.5 Software Installation: All IT platforms shall have a documented list of approved software as part of the configuration baseline and be configured to restrict the installation of prohibited or unauthorized software.

200.1.6 Secure Software Development: Secure software development practices such as the Secure Software Development Framework (SSDF) and the Software Assurance Maturity Model (SAMM) shall be integrated, and security monitored, throughout the software development life cycle.

200.1.7 Cybersecurity Inventory Management: All IT platforms shall maintain a master inventory that ties IT assets to the security controls protecting them.

Table 1 RACI Matrix – Platform Security

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Configuration Management	C	I	A	R	C
SW Security	C	I	A	R	C
HW Security	C	I	A	R	C
Audit Logs	C	I	A	R	C
SW Installation	C	I	A	R	C
SW Development	C	I	A	R	C
Cybersecurity Inventory Management	C	I	A	R	C

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

200.2 INFRASTRUCTURE SECURITY

200.2.1 Network Security: All IT networks and cloud-based platforms shall be logically segmented according to trust boundaries and platform types (e.g., IT, IoT, OT, mobile, guests) and permit only the required and authorized communications between segments. Where feasible, agencies shall implement both macro-segmentation and micro-segmentation strategies to reduce the attack surface, limit lateral movement, and protect data confidentiality, integrity, and availability across all networks.

200.2.2 Environmental Protection: All IT networks shall be protected from environmental threats (e.g., fire, flooding, heat, humidity).

200.2.3 Resilience: All systems, infrastructure, and control mechanisms (e.g., load balancing, redundant storage) shall be implemented to avoid single points of failure and withstand and quickly recover from disruptions, whether caused by cyberattacks, hardware failures, or natural disasters. Agencies shall implement a geographically dispersed architecture where it is feasible to support resilience across critical systems, services, and data assets.

200.2.4 Capacity Management: Usage of storage, power, compute, network bandwidth, and other resources shall be monitored to adequately forecast needs, scale resources accordingly, and maintain availability.

Table 2 RACI Matrix – Infrastructure Security

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Network Security	C	I	A	R	C
Environmental Protection	C	I	A	R	C
Resilience	C	I	A	R	C
Capacity Management	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

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.PS: Platform Security	Section 200.1
Protect	PR.IR: Technology Infrastructure Resilience	Section 200.2

[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**.