DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

Access Control 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

ACCESS CONTROL POLICY

MD-POL-204-01 **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

ACCESS CONTROL POLICY

MD-POL-204-01 | **Last Updated: 02/18/2026**

100 INTRODUCTION

Purpose:	This policy establishes a framework for managing and safeguarding access to State information systems and resources.
Scope:	This policy defines organizational access controls 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Superseded Policy:	The full policy suite outlined in MD-POL-100 Cybersecurity & Governance Policy, Appendix C supersedes the State of Maryland Information Technology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.
	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.
	Data Custodian (DC): An individual or organization responsible for the safe custody, transport, and storage of data assets.
	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, or network service 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 State's cybersecurity access control policy. Access control contributes to a Zero Trust Architecture (ZTA) by ensuring that users, devices, and applications are continuously verified before being granted access to resources.

200.1 IDENTITY MANAGEMENT

All agencies shall implement technologies that give authorized users appropriate access to State resources in accordance with the following policy:

200.1.1 Identity Management: Identities and credentials for authorized users, services, applications, and hardware shall be managed (including privileged and non-privileged accounts) in accordance with the DoIT-approved standards. Identities shall be unique, persistent, and never reused.

200.1.2 Identity Verification: Identities shall be proofed and bound to credentials (e.g., State-issued identity credentials) and resolve user identities to a unique individual.

200.1.3 Modern Authentication: Identities and credentials for authorized users, services, applications, and hardware shall be authenticated using modern technologies. Modern technologies include multi-factor authentication (MFA), passwordless authentication, certificate-based authentication, or hardware tokens/smartcards. Where feasible, organizations should implement continuous authentication supported by phishing-resistant MFA to ensure identity verification occurs at every stage of a user's interaction, not solely during login.

200.1.4 Identity Assertions: Identity assertions, including user ID, authentication method, timestamp, roles, or other attributes, shall be protected (e.g., digitally signed, encrypted) and verified to ensure integrity and confidentiality. Assertions are often encoded in standards like SAML, OAuth ID Tokens, or OpenID Connect.

Table 1 RACI Matrix - Identity Management

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs
Identity Management	C	I	A	R	C
Identity Verification	C	I	A	R	C
Authentication	C	I	A	R	C
Identity Assertions	C	I	A	R	C

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

200.2 ACCESS MANAGEMENT

All agencies shall manage and enforce access permissions and authorizations in accordance with the following policy:

200.2.1 Access Control: Access to digital assets (e.g., files, databases, applications), logical assets (e.g., systems, cloud services, network segments), and mobile devices (e.g., smartphones, tablets, and other portable endpoints running iOS, Android, or Google-managed platforms) shall be limited to authorized users, services, and hardware, and shall be actively managed in accordance with organizational access policies.

200.2.2 Account Terminations: Access rights of all users shall be removed upon termination of their employment, association with the State of Maryland, or adjusted as appropriate upon changes in role. All non-human identities (e.g., including service accounts, automated agents, scripts, and robotic process automation (RPA) entities) shall also be disabled when:

- The associated system, application, or process is decommissioned;
- The identity is no longer required for operational purposes;
- Ownership or accountability cannot be verified; or
- The identity poses a security or compliance risk.

Accounts may be fully removed or terminated once data retention and legal requirements are satisfied.

200.2.3 Principle of Least Privilege: Access to State systems shall be restricted to the minimum access and privileges necessary in line with Zero Trust principles.

200.2.4 Separation of Duties: System access authorizations shall be defined to support the division of critical functions and responsibilities. This prevents any single individual from having unchecked authority over critical processes.

200.2.5 Physical Access: Physical access to assets shall be managed, monitored, and enforced commensurate with risk.

200.2.6 Foreign Travel with State IT: Traveling outside the United States and its Territories with State equipment must be pre-approved. Requests may be denied due to elevated cybersecurity risk conditions, U.S. export laws or import restrictions enforced by the destination country. For approved requests, a set of security configuration requirements as well as post-travel requirements will be defined and shall be adhered to.

Logins or access to State Data from outside the United States and its Territories will be denied by default. Access is granted on an as-needed basis following approval of the appropriate AO or System Owner.

Table 2 RACI Matrix – Access Management

	DOIT	SCISO	Secretaries / Directors	IT Managers	ISOs
Access Control	C	I	A	R	C
Account Terminations	C	I	A	R	C
Principle of Least Privilege	C	I	A	R	C
Separation of Duties	C	I	A	R	C
Physical Access	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.AA: Identity Management, Authentication, And Access Control	Section 200.1 Identity Management Section 200.2 Access Management

[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**.