DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

Asset 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

ASSET MANAGEMENT POLICY

MD-POL-202-01	Last Updated: 02/18/2026

100 INTRODUCTION

Purpose:	This policy establishes the requirements for identification and management of all information technology (IT) assets consistent with their relative importance to the State.
Scope:	This policy applies to all State-owned and operated IT assets (including hardware, software, and data) that generate, receive, store, process or transmit State data.
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Superseded Policy:	The full policy suite outlined in MD-POL-100 Cybersecurity & Governance Policy, Appendix C supersedes the State of Maryland Information Technology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.
	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 establish requirements for identifying, documenting, classifying, and maintaining an accurate and authoritative inventory of all State systems and assets throughout their lifecycle. These requirements ensure continuous visibility, ownership accountability, and risk-informed protection of assets that store, process, or transmit State information or connect to State networks.

200.1 INVENTORY BASELINES

All agencies shall implement and strictly enforce the following asset management activities:

200.1.1 Hardware: Develop, document, and maintain a centralized inventory of all hardware devices including IT, network devices, Operational Technology (OT), Internet of Things (IoT), and mobile devices.

200.1.2 Software: Develop, document, and maintain a centralized inventory of all types of software and services, including commercial-off-the-shelf, open-source, custom applications, application programming interface (API) services, and cloud-based applications and services.

200.1.3 Virtual Assets: Develop, document, and maintain a centralized inventory of virtual machines, containers, and cloud instances including their hosting platforms and resource allocations.

200.1.4 Data: Develop, document, and maintain a centralized data asset inventory as directed by the Office of Enterprise Data (OED), SCDO, Agency Data Officers (ADO), and State Data Governance guidelines. Where feasible, agencies shall use automated means for data discovery, data labeling, and tagging.

200.1.5 Data Model: Develop and document, within the System Security Plan (SSP), a data model that depicts a baseline of communication and data flows, both internal and external, including all system interconnections and the expected network ports, protocols, and services used by authorized systems, with updates required upon significant system, network, or data handling changes.

200.1.6 Asset Labeling: Apply standardized labels or tags to each IT asset to indicate its business value, regulatory obligations, and operational role. This labeling focuses on categorizing and marking assets, not defining data classification.

Table 1 RACI Matrix – Inventory Baselines

	DOIT	SCISO/ SCDO/SCPO	Secretaries/ Directors	IT Managers	ISO
Hardware	I	C	A	R	C
Software	I	C	A	R	C
Virtual Assets	I	C	A	R	C
Data	I	C	A	R	C
Data Flow	I	C	A	R	C
Classification	I	C	A	R	C

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

200.2 LIFECYCLE MANAGEMENT

200.2.1 Inventory Monitoring: Each agency is responsible for the management of accurate inventories over the life of each system. Continuously monitor for changes in inventory such as:

- Transfer of systems, hardware, software, services, and data within the organization;
- New inventory items;
- Software and service inventory changes (e.g., platforms including containers and virtual machines for software and virtual asset inventory changes);
- New external services such as third-party infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings; serverless functions; container registries; APIs and API gateways; hybrid cloud interconnections; and other externally hosted application services;
- Cloud resource sprawl monitoring and cost optimization tracking;
- Introduction of new data types; and
- Unsupported (i.e., end-of-life or end-of-service) software and hardware requiring replacement.

Table 2 RACI Matrix – Lifecycle Management

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISO
Inventory Monitoring	C	I	A	R	C

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

Refer to MS-STD-317-SA System & Services Acquisition Standard for more information about integrating security requirements into new asset procurements including cloud services.

200.3 ZERO TRUST ENFORCEMENT

In alignment with the State's ZTA strategy, agencies shall begin integrating asset management with Identity and Access Management (IAM) wherever possible. Examples of key strategies:

- Automatically identifying and categorizing assets by IT type and by business criticality to apply IAM policies correctly;
- Implementing automated asset discovery tools that integrate with identity management systems;
- Assigning permissions based on asset type, user role, and security requirements;
- Establishing device certificates and attestation mechanisms for hardware authentication;
- Ensuring assets are continuously verified before granting access;
- Managing asset access dynamically based on user status and security posture;
- Implementing real-time asset-health monitoring to inform access decisions;
- Restricting access based on contextual risk assessments, ensuring least privilege access; and
- Triggering automated incident response procedures when unauthorized or compromised assets are detected.

Table 3 RACI Matrix – Zero Trust Enforcement

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISO
Monitoring	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
Identify	ID.AM: Asset Assessment	Section 200.1 Inventory Baselines Section 200.2 Lifecycle 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**.