DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

IT Acceptable Use 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

IT ACCEPTABLE USE POLICY

MD-POL-203-01	Last Updated: 02/18/2026

100 INTRODUCTION

Purpose:	This policy establishes allowances and conditions for the acceptable use of State-owned or State-managed IT assets.
Scope:	This policy 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Superseded Policy:	The full policy suite outlined in MD-POL-100 Cybersecurity & Governance Policy, Appendix C supersedes the State of Maryland Information Technology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.
	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 acceptable use requirements for protecting and handling State data and State assets.

200.1 ACCEPTABLE CONDUCT

200.1.1 Authentication Policy: Users shall follow all authentication practices defined by DoIT for State identity management, including required password standards and multi-factor authentication procedures.

200.1.2 Cybersecurity Awareness: Using State-owned IT resources in a safe and responsible manner is required of all users. All users are required to complete assigned Security and Privacy Awareness Training within the timeframe allocated. If training is not completed within the timeframe allotted, the impacted individual's State account may be disabled.

200.1.3 State-Managed Social Media: Only authorized personnel may post to State-managed social media accounts. Only public data may be posted on State-managed social media accounts. Non-Public State information must never be shared, stored or exchanged on social media platforms.

200.1.4 Personal Social Media: Personal social media shall not be accessed from Maryland systems including state issued phones unless explicitly authorized by the appropriate agency executive (e.g. Authorizing Official, Data Owner). Social media services that have developmental and strategic origins from other countries, or have versions that operate outside of the U.S., shall not be used on Maryland systems or state issued mobile devices.

200.1.5 Text Messages: State business shall only be conducted on State issued email, Google or Teams chat or other State communication system authorized by DoIT. These systems are governed by cybersecurity and privacy policies and standards.

200.1.6 Data Handling: Users must handle State data according to the security protections defined by the business, system, and data owners in alignment with the State Data Classification Policy and any Data Use or Data Sharing Agreements that are in place between organizations.

200.1.7 Secure Remote Access Usage: All personnel must use secure remote access, in alignment with the State-approved network security architecture, whether that be through a Zero Trust Network Access (ZTNA) mechanism or a Secure Access Service Edge (SASE) service, at all times when accessing State systems, data, or services from any location outside the secured internal State network. This requirement applies to all remote, hybrid, and mobile access scenarios, including use of laptops, tablets, and smartphones.

200.1.8 Emerging Technologies: Emerging technologies (e.g., artificial intelligence (AI) powered solutions, machine learning, blockchain, quantum computing, Internet of Things (IoT)) shall not be used for official State business without a risk assessment, approval from the SCISO, and authorization under a formal agency-level policy.

200.1.9 Reporting Suspicious Activity: All users are required to promptly report any security and privacy violations or suspicious activities (within **1 hour** of discovery) to DoIT. This includes, but is not limited to:

- Unauthorized access to or use of information systems;
- Attempts to bypass system protections;
- Detection of malware, phishing attempts, or other cyber threats;
- Unusual system behavior that may indicate a security breach; and
- Suspicious (or known) incident impacting non-public data (Data Classification Level 2 or above).

Reporting Methods

Reporting Form	Email	Phone
https://doitmaryland.service-now.com/cybersecurityincident/	SOC@maryland.gov	410-697-9700-option #5

Table 1 RACI Matrix – Expected Security Behaviors

	DOIT	SCISO/ SCPO	Secretaries/ Directors	IT Managers	ISOs	Users
Authentication Policy	C	I	A	C	-	R
Cybersecurity Awareness	C	I	A	C	-	R
State-Managed Social Media	C	I	A	C	-	R
Personal Social Media	C	I	A	C	-	R
Text Messages	C	I	A	C	-	R
Data Handling	C	I	A	C	-	R
VPN Usage	C	I	A	C	-	R
Emerging Technologies	C	I	A	C	-	R
Reporting Suspicious Activity	C	I	A	C	-	R

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

200.2 UNACCEPTABLE CONDUCT

200.2.1 Harassment: Any form of cyberbullying, harassment, inappropriate language, or discrimination in any State communications and interactions is strictly prohibited.

200.2.2 Unauthorized Access: Unauthorized access, duplication, storage, manipulation, disclosure, transfer, use, or release of State Information or State systems including cloud systems and infrastructure is prohibited.

200.2.3 Password Reuse: In accordance with Maryland IT standards, IT users will not be permitted to use the same password across multiple accounts. User shall never use the same password for both personal email and their State login credentials.

200.2.4 Password Protection: Passwords must not be stored in unencrypted files, written down, or shared verbally. Use of approved password managers is strongly encouraged for password management. Approved password managers are required for password management of application or device root passwords, database encryption keys and similar state resources. Suspected password compromise must be reported immediately.

200.2.5 Personal Email: IT users are prohibited from creating alternate email accounts through public email service providers (e.g., Gmail, Hotmail, Yahoo, Outlook, iCloud, AOL, Comcast) with any reference to the State by name, facility, agency, or Department.

200.2.6 Shared Passwords: Every user and system shall be issued a unique user identification and password to access State IT assets. Sharing passwords among users or disabling multi-factor authentication is strictly prohibited.

200.2.7 Mobile Devices: Personally owned mobile devices (e.g., smartphones, tablets, and other portable endpoints running iOS, Android, or Google-managed platforms) may not be used to access State systems, unless explicitly authorized by the agency's designated authorizing official. Where explicitly authorized, users must maintain technical and administrative safeguards defined by DoIT.

200.2.8 Software: State-issued software may not be modified or reconfigured. Downloading software that is not explicitly authorized by DoIT is prohibited. Uploading of State-owned software to external content repositories that have not been authorized by DoIT is prohibited.

The following capabilities are restricted to authorized security personnel. End users are strictly prohibited from accessing, executing, or attempting to use these tools under any circumstances.

Category	Applications
Anti-Forensic	Anti-forensic and technologies designed to obstruct digital investigations.
Hacking	Tools designed for gaining unauthorized access or tools capable of disrupting operations or services.
Administration	Remote access / administration tools.
Encryption	Tools capable of locking the State out of needed data.

200.2.9 Hardware: Any modification to State-issued hardware or use of hardware that is not provided by the State must be approved by DoIT. Hardware components are included within the scope of this policy when they require drivers or supporting software that could affect the State's security posture. Examples include: Bluetooth-enabled accessories, biometric readers, external network adapters, printers or scanners that install drivers, and any smart or IoT-enabled hardware that requires supporting software to function.

200.2.10 Removable Media: Personally owned removable media such as external hard drives, Universal Serial Bus (USB) devices, and other removable storage media are strictly prohibited. State-owned removable media is not permitted unless the exception is explicitly approved by the appropriate agency AO and only for business needs or processes that

cannot make use of State-authorized email, cloud storage, and file transfer services. If the exception is approved, the user must comply with DoIT standards regarding encryption, safe handling, asset tracking and data backups.

200.2.11 Cloud Services: Users shall not make use of any Software as-a-Service (SaaS) solutions (i.e., cloud-hosted applications delivered over the internet) and Platform-as-a-Service (PaaS) solutions (i.e., cloud-based application development and deployment environments) for State business that has not been evaluated by DoIT for compliance with published State IT security policy, regulatory requirements, and DoIT technology standards prior to acquisition.

200.2.12 Artificial Intelligence: AI products, services, or tooling may not be used with non-public data (i.e., Data Classification Level 2 or above) unless approved by the appropriate agency AO and Data Owner. Use cases shall be reviewed for compliance with data protection policies and assurance that the tool is not exposing non-public data for external model training (i.e., utilizes a private tenant). When an AI use case is approved, users shall comply with the mandatory conditions that govern its use as defined by approver.

Table 2 RACI Matrix – Unacceptable Behavior

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs	Users
Harassment	C	I	A	C	-	R
Unauthorized Access	C	I	A	C	-	R
Password Reuse	C	I	A	C	-	R
Password Protection	C	I	A	C	-	R
Personal Email	C	I	A	C	-	R
Shared Passwords	C	I	A	C	-	R
Mobile Devices	C	I	A	C	-	R
Software	C	I	A	C	-	R
Hardware	C	I	A	C	-	R
Removable Media	C	I	A	C	-	R
Cloud Services	C	I	A	C	-	R
Artificial Intelligence	C	I	A	C	-	R

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

200.3 PERMITTED USE OF STATE-OWNED IT ASSETS

200.3.1 Business Use: State data and IT resources are provided to the State workforce for the purpose of producing work product and conducting official business.

200.3.2 Limited Personal Use: Personal use of State-owned IT is permitted on a limited basis only and for reasonable purposes that would otherwise be difficult to perform outside of normal business hours (e.g., communicating with family members during an emergency, visiting trusted websites to review appointment times). Users shall have no expectation of privacy when using State IT assets.

200.3.3 International Travel with State IT Assets: 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.

200.3.4 State Email: State email service is provided as a tool for use in connection with State business purposes. State email accounts may only be provisioned by DoIT. Any confidential and restricted data (Data Classifications Level 3 or above) transmitted via email externally must be encrypted using State-provided encryption tools. Follow agency standards for enabling additional encryption methods beyond the default protection afforded by State email.

200.3.5 Inactivity Logout: State personnel are expected to take physical action to log out when they are expecting inactivity longer than 15 minutes to prevent idle sessions that are vulnerable to unauthorized access.

Table 3 RACI Matrix – Permitted Use of State IT Assets

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs	Users
Business Use	C	I	A	C	-	R
Limited Personal Use	C	I	A	C	-	R
International Travel with State IT Assets	C	I	A	C	-	R
State Email	C	I	A	C	-	R
Inactivity Logout	-	-	-	C	-	R

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

200.4 PROHIBITED USE OF STATE IT ASSETS

200.4.1 Illegal Activity: State data and IT resources may not knowingly be used for any illegal, harmful, fraudulent, infringing, or offensive use such as cyberbullying, harassment, inappropriate language and discrimination or to transmit, store, display, distribute, or otherwise make available content or software applications that could cause harm to the State.

200.4.2 Malicious Activity: Users shall not access, or attempt to access, any State resources to which an individual is not authorized to access. Individuals are further prohibited from the following.:

- Unauthorized Access: Any attempt to read, modify, store, or delete any State data or software located anywhere in the State's IT resources to which the user does not have authorized access.
- IT Reconfiguration: Any attempt to interfere with or tamper with the normal operation of State-provided IT resources, or to otherwise interfere with the operation of the State's IT resources; and any attempt to alter or change the standard State-configuration of an application or a device's security feature, or to circumvent security features, such as requirements, endpoint protection settings without SCISO review and approval. Examples of IT reconfiguration include but are not limited to distribution of unsolicited advertising; propagation of computer viruses; and attempted use of the network for gaining unauthorized entry to equipment or resources accessible through the State IT network.
- Impersonation: Any attempt to assume the identity of any other person, by use of a username or ID that is not assigned to the user or by attempting to determine a password by any means.
- P2P File Sharing: The use of Peer-to-Peer (P2P) software, or any file sharing technology, that violates the rights of any person or company protected by copyright, trade secret, patent or other intellectual property.
- Monitoring: Conducting any form of network monitoring, scanning, or penetration testing without approval from the SCISO.

200.4.3 Unauthorized Internet Activity: The State's internet service is provided as a resource for conducting official business. The following internet use is prohibited:

- Illegal Activity: Using the Internet or WIFI service to access or transmit any material that violates any applicable local, state, national or international law, or any rule or regulations promulgated thereunder is prohibited.

- Downloads: Downloading software applications or executable content from the internet, email, or social media is prohibited unless the source is a trusted and it is a contractually authorized vendor. All software must be evaluated by DoIT (or as delegated to individual approvers within each agency) prior to initial use. Subsequent updates or patches from authorized vendors may be retrieved via secure internet portals or email in accordance with the System Security Plan (SSP).
- Streaming: Accessing high bandwidth video content and media platforms from the State network is not permitted unless required to perform assigned job duties.

200.4.4 Personal Email for State Work: Conducting any State business using a Non-State-issued, personal email account is prohibited.

200.4.5 Accessing Personal Email from State Systems: Accessing personal email accounts (e.g., Gmail, Hotmail, Yahoo, Outlook.com, iCloud, AOL, Comcast) from a State network or State-issued device is prohibited given the risk it presents of introducing malware to the State IT environment.

200.4.6 Email Forwarding: Manual or auto-forwarding of State email to a third-party email system (e.g., personal email account) is prohibited unless an exception request is approved by DoIT.

200.4.7 File Sharing: Use of private file sharing services (e.g., Google Drive, iCloud, Dropbox) and any unapproved technology to store or transmit State data such as work products, artifacts, and business tools is prohibited. State approved file sharing services are those that have been securely configured and registered by DoIT for enterprise use, or by the agency for agency-specific services.

200.4.8 Online Collaboration: State-authorized collaboration tools may be used for video conferencing, online meetings, and chat in accordance with DoIT published technology standards. External participants will be provided only the minimum access needed to meet the needs of the agency for online collaboration.

Table 4 RACI Matrix – Prohibited Use of State IT Assets

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs	Users
Illegal Activity	C	I	A	C	-	R
Malicious Activity	C	I	A	C	-	R
Internet Activity	C	I	A	C	-	R
Personal Email for Work	C	I	A	C	-	R
Accessing Personal Email From Work	C	I	A	C	-	R
Email Forwarding	C	I	A	C	-	R
File Sharing	C	I	A	C	-	R
Online Collaboration	C	I	A	C	-	R

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

200.5 OVERSIGHT & GOVERNANCE

200.5.1 Monitoring: DoIT reserves the right to audit networks, devices, and systems on a continuous, periodic, or ad-hoc basis; The Department of IT may perform network scans and monitor equipment, systems, and network traffic at any time, without notice.

200.5.2 Technology Standards: Users shall comply with DoIT-approved standards on the acceptable use of approved products, features, and any required configurations as deemed necessary to mitigate risk.

200.5.3 User Agreement: All new users are required to read, understand, and acknowledge the State's Acceptable Use Policy before being granted access to any IT resources; and all users are required to periodically re-acknowledge the AUP when requested.

Table 5 RACI Matrix – AUP Oversight & Governance

	DOIT	SCISO	Secretaries/ Directors	IT Managers	ISOs	Users
Monitoring	R	A	I	R	C	-
Technology Standards	R	A	I	I	C	-
User Agreement	C	C	A	C	C	R

[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
Govern	GV.RR: Roles, Responsibilities, and Authorities	Section 200 Policy
Govern	GV.PO: Policy	Section 200 Policy
Identify	ID.IM: Improvement	Section 200.5 AUP Oversight & Governance
Identify	ID.IM: Improvement	Section 200.5 AUP Oversight & Governance
Identify	ID.IM: Improvement	Section 200.5 AUP Oversight & Governance
Identify	ID.IM: Improvement	Section 200.5 AUP Oversight & Governance
Identify	ID.IM: Improvement	Section 200.5 AUP Oversight & Governance
Protect	PR.AA: Identity Management, Authentication, and Access Control	Section 200.1.1 Authentication Policy
Protect	PR.AT: Awareness and Training	Section 200.1.2 Cybersecurity Awareness
Protect	PR.DS: Data Security	Section 200.1.4 Data Handling

[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**.