State of Maryland

STANDARD

ACCESS CONTROL

Document No.	Last Updated	Prepared By
MD-STD-301-AC-01	02/18/2026	DOIT OSM

Access control, as a core principle of Zero Trust Architecture (ZTA), is crucial for safeguarding State data, resources, and systems by ensuring that only authorized users, validated through continuous verification, can access specific information or functions.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to manage access to systems, applications, and data.
Scope	This standard establishes an organizational approach for access control and is not specific to any single platform or technology solution.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as "agencies."
Related Policy	This standard is part of a broader policy suite. Refer to MD-POL-100 Cybersecurity & Governance Policy, Appendix C for a list of related policies and standards.
Baseline	This standard has been developed using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 Moderate Baseline[1] and State-specific organizationally defined parameters. Agencies may be required to deviate from this baseline when State statute, executive orders, or applicable regulations establish a conflicting requirement that precludes compliance.
Distribution	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.

[1] NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

FOREWORD

Agencies that use Department of Information Technology DoIT-managed services automatically receive, or *inherit*, the compliance those services already meet, reducing duplicative work and accelerating their overall compliance efforts. These centrally governed services, such as hosting platforms, identity management, and network infrastructure, are built with robust control frameworks that automatically extend to participating agencies. By leveraging these offerings, agencies not only align with key operational and security standards but also benefit from pre-configured environments, continuous monitoring, and policy enforcement mechanisms maintained by DoIT. Agencies are encouraged to leverage these services to accelerate readiness, gain cost efficiency, simplify compliance efforts, and allow agencies to focus more fully on mission delivery, knowing that foundational requirements are already in place. Agencies should review the scope of each managed service to understand which standards are inherited and where additional agency-specific controls may still be required.

GUIDANCE AND ENFORCEABILITY

Throughout this document, informational call-out boxes are utilized to provide additional context or elaborate on key topics. While these boxes primarily serve an informational purpose, any directives or mandated actions contained within them are authoritative and carry the same enforceability as the core requirements of this document. For the purposes of this document, the term “shall” denotes a mandatory requirement. Terms such as “where feasible”, “encouraged”, or similar phrasing indicate recommended practices that reflect organizational preference but are not enforceable requirements at this time.

CHANGE RECORD

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

STANDARDS

301 State Strategy

These standards establish a baseline of access control practices that each agency must implement to comply with State cybersecurity and privacy policies. Each agency shall designate specific personnel with IT responsibilities to ensure the effective implementation of these standards.

301-1 Develop Agency-Level Procedures (AC-1)

In alignment with this standard, develop and document agency-level access control procedures. Agencies must disseminate the procedures to agency personnel with information technology (IT) security responsibilities. Agencies must review, and if needed, update the procedures as deemed appropriate by the agency based on changes and risk at least every **3 years**. At a minimum, the procedures must address purpose, scope, roles and responsibilities, and guidelines.

301-2 Manage System Accounts (AC-2)

Manage all system accounts (i.e., individual, system, guest, anonymous, emergency, developer, temporary, and service accounts) as follows**:**

- Define and document the types of accounts allowed and specifically prohibited for use within the system. At a minimum, guest/anonymous accounts shall not be permitted, and access shall be limited to individuals and non-human identities with a valid business purpose.
- Assign account managers for each agency-managed system.
- Establish agency/system-specific conditions for group and role assignment.
- Identify authorized users of the information system specifying group role assignment, access authorizations (i.e., privileges), and define system-specific attributes (as required) for each account.
- Create, enable, modify, disable, terminate and remove information system accounts in accordance with agency-level procedures.
- Monitor the use of accounts.
- Notify account managers when accounts are no longer required; when users are terminated or transferred; and when system usage or need-to-know changes for an individual.

- Authorize access to the system based on a valid access authorization, intended system usage, and system-specific attributes or rules of behavior as required by the agency’s business functions.
- Review accounts for compliance with account management requirements at least **annually**; Privileged accounts shall be reviewed at least **semiannually**.
- Prohibit the use of shared accounts (i.e., shared logins) and generic accounts unless explicitly authorized by the appropriate Authorizing Official (AO).
- Maximize account monitoring through continuous or near-real-time observation and assessment.
- Where feasible, deploy Privileged Access Management (PAM) solution for enhanced access control and privilege escalation.

Context-Aware Access Control

A key implementation strategy within ZTA is the use of granular, dynamic access controls such as: a) Need-Based Access: Users are granted access only to the resources necessary for their specific roles or tasks, minimizing the attack surface and limiting lateral movement in the event of a breach; b) Session-Based Access: Access is granted for a defined session duration, ensuring that permissions are not persistent and reducing the risk of unauthorized reuse; and c) Just-in-Time (JIT) Access: Privileged access is provisioned only when needed and for the shortest possible time, helping prevent standing privileges that could be exploited by malicious actors or insider threats. These controls are especially critical for privileged access requests, where elevated permissions could lead to significant security risks if misused.

AC-2(1): Support the management of system accounts using automated mechanisms such as:

- Provisioning systems via Identity and Access Management (IAM) platforms;
- Notification systems such as email and IAM platforms;
- Access reviews using governance tools;
- Deactivation triggers using automation/scripts; and
- Usage monitoring using Security Information and Event Management (SIEM) platforms.

AC-2(2): Disable temporary and emergency accounts, automatically, manually, or combination thereof, within **24 hours** (including Federal and State holidays) of the designated temporary access period. The designated temporary access period shall be limited to a maximum number of days driven by risk for each use case.

AC-2(3): Disable accounts within **24 hours** when the accounts: a) have expired; b) are no longer associated with a user or individual; c) are in violation of organizational procedures; or d) have been inactive for **30 days**. New accounts that are not used within the first **30 days** will be disabled.

AC-2(4): Automatically audit account creation, modification, enabling, disabling, and removal actions using a combination of system logging and event monitoring and notification mechanisms.

AC-2(5): Require that users log out when expected inactivity will exceed **15 minutes** (e.g., workstations, laptops, web applications).

AC-2(13): Disable accounts of individuals immediately upon discovery of significant risk. Risk level is determined by evaluating impact severity, likelihood, and scope of harm, and risk tolerance is defined by the appropriate AO.

301-3 Enforce Authorized Access (AC-3)

Enforce approved authorizations for logical access to information and system resources in accordance with agency-level procedures, change all default manufacturer passwords, and give only authorized personnel access to the stored configuration files.

For any system, software, or service procured and managed by an agency under the purview of Office of Security Management (OSM), access shall be provided to OSM that permits visibility into system, application, or service configuration and logs to facilitate timely incident response support.

Zero Trust Architecture

Where feasible, implement policy-based access control (PBAC) using ZTA design principles that enable dynamic, context-aware authorization that adapts to evolving threats and operational needs. Implementing PBAC using ZTA design principles means that access decisions are no longer based on static roles or network location. Instead, they are dynamically enforced through context-aware policies that evaluate who is requesting access, what they are trying to access, and under what conditions. (i.e., Attribute-based access control (ABAC), JIT access, and PAM).

301-4 Control the Flow of Information (AC-4)

Enforce approved authorizations for controlling the flow of information within the system and between connected systems, based on agency-level procedures using methods such as boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content. These configuration settings shall be reviewed at least **annually**.

Flow Control Restrictions

Flow control restrictions refer to policies and mechanisms that regulate how data moves between systems, users, and environments, especially across trust boundaries. Examples of flow control restrictions include: a) No management interfaces for any State devices accessible over the public internet; b) Blocking outside traffic that claims to be from within the organization; c) Validating that all device management sessions come from authorized Internet Protocol (IP) addresses/subnets from the internal network; and d) Limiting information transfers between organizations to those that are required for mission or business needs and approved based on the risk determinations and tradeoffs made by the AO.

301-5 Maintain Separation of Duties (AC-5)

Identify and document the duties of agency individuals requiring separation, to prevent malevolent activity without detection or accountability, and define system access authorizations to support separation of duties as follows:

- Define information system access authorizations to support separation of duties.
- Effectively segregate duties between the administration functions and the auditing functions of each system.
- Have separate Administrator accounts for system and network administrators who require specific, elevated privileges to perform their job functions.
- Maintain separation among the following four (4) categories of “duty” or employ compensating controls to monitor activity closely:

Separation of Duties

Role	Purpose
IT Administration (or Operation)	Assuring systems function, to serve the system users.
IT Access Management	Account creation, modification, removal, etc.
IT Security	Assuring adequacy of system controls for availability, integrity, and confidentiality.
IT Management	Allocating adequate resources for implementation of effective information security programs and system controls.

301-6 Employ the Principle of Least Privilege (AC-6)

Allow access only for authorized users, non-human identities, or processes acting on behalf of users when such access is necessary to perform assigned duties consistent with position descriptions, agency missions, and business functions. Agencies must, at a minimum:

- Validate and inventory all accounts;
- Minimize the number of privileged accounts;
- Limit functions that can be performed using remote access;
- Limit the duration that privileged users can be logged in based on risk; and
- Log privileged user activities and review the logs regularly.

AC-6(1): Explicitly authorize agency personnel responsible for establishing system accounts, configuring access authorizations (e.g., permissions, privileges), defining auditable events, and setting intrusion-detection parameters.

AC-6(2): Require that users of administrative accounts, or system accounts (or roles) with access to security functions or security relevant information (e.g., establish system accounts, configure access permissions, modify audit settings and intrusion detection parameters) use non-privileged accounts or roles, when accessing non-administrative or non-security functions.

AC-6(5): Restrict privileged accounts on systems to agency-authorized system administrators. Note: Personnel who no longer require this level of access must be promptly removed from the approved access list.

AC-6(7): Review **quarterly** the privileges assigned to system administrators and security personnel to validate the need for such privileges and reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AC-6(9): Log and audit the execution of privileged functions. Auditing the use of privileged functions using PAM solutions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

AC-6(10): Prevent non-privileged users from executing privileged functions to include at a minimum:

- Disabling, circumventing, or altering implemented security safeguards/countermeasures.
- Creating, modifying and deleting user accounts and groups.
- Granting, modifying, and removing file or database permissions.
- Configuring authentication and account lockout system-level policy.

- Configuring system-level policy regarding the number and length of sessions.
- Changing authenticators or certificates of users other than oneself.
- Determining how the application will respond to error conditions.
- Determining auditable events and related parameters.
- Establishing log sizes, fill thresholds, and fill behavior (e.g., action when the log is full).

301-7 Enforce Limits on Unsuccessful Logon Attempts (AC-7)

Enforce a **limit of 3-5** consecutive invalid logon attempts by a user during a **30-minute** time period and automatically lock the account or node for a minimum of **15 minutes** or until released by an administrator/authorized account manager.

Set login delay between login prompts after a failed login to **4 seconds or greater** and notify system administrator/authorized account manager when the maximum number of unsuccessful attempts is exceeded.

Zero Trust Architecture

Where feasible, use risk-based adaptive lockout thresholds for agencies with modern IAM capabilities. A risk-based adaptive lockout threshold is a dynamic security control that adjusts how and when user accounts are locked out based on the perceived risk of the login attempt, rather than using a fixed number of failed attempts across all scenarios. An example of this in practice is a smart lockout feature.

301-8 Display System Use Notification (AC-8)

Display the approved system use notification message for all interactive logon interfaces, before granting access to any system, to disclose privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

Where feasible, include an agency-approved system use notification message for non-interactive access (i.e., Application Programming Interfaces (APIs), system accounts) where a risk assessment deems it necessary.

Approved Banner: Any deviation from this official banner shall be approved by DoIT.
"WARNING! This system is a State of Maryland information system, which may contain State information and is restricted to authorized users only. Unauthorized access, use, misuse, or modification of this information system; the data contained herein; or data in transit to or from this system constitutes a violation of Maryland Criminal Law Article §§ 7-302 and 8-605 through 8-611, and Title 18, U.S.C. § 1030 (Computer Fraud and Abuse Act). Violators may be subject to criminal and civil penalties. **This system and its equipment are subject to monitoring to ensure the proper performance of applicable security features and procedures. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel. Anyone using this system expressly consents to such monitoring."**

For publicly accessible systems: a) Display the system use information before granting access to the publicly accessible system; b) Display references, if any, to monitoring, recording, or auditing that are consistent with special privacy rules or constraints for such systems that generally prohibit those activities; and c) Include a description of the authorized uses of the system in the notice.

301-9 Require Device Lock (AC-11)

Prevent access to the system by initiating a device lock after **15 minutes** of inactivity or upon receiving a request from a user and requiring the user to initiate a device lock before leaving the system unattended. Retain the device lock until the user re-establishes access using established identification and authentication procedures. "Inactivity" is defined as the absence of user-initiated actions; system and application processes are excluded.

AC-11(1): Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

301-10 Automatically Terminate Sessions (AC-12)

Limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications to a **single session** to minimize the risk of session hijacking or unauthorized access.

Automatically terminate general user sessions after **15 minutes** of inactivity, and privileged users after **5 minutes** of inactivity, or as determined by the AO as acceptable from a risk perspective. Commercial off-the-shelf (COTS) or custom applications are required to terminate network connections at the end of a session or due to inactivity.

301-11 Identify all System Actions Permitted Without Identification or Authentication (AC-14)

Identify and document any actions (system or user initiated) that can be performed on the system without identification or authentication as approved by the agency AO based on risk.

Examples of Approved Unauthenticated Actions

There are very limited circumstances where unauthenticated access would be considered acceptable to an agency AO: a) Displaying public-facing content to constituents (e.g., login banner, help page, or terms of use) with no access to non-public State data; b) IT administrators running scheduled maintenance scripts that don't access non-public State data; c) Public viewing of system status indicators (e.g., "System Online") on a kiosk; d) Sending heartbeat signals to authorized monitoring tools (e.g., no user interaction; telemetry only); and e) Constituent submitting a contact form or feedback without login (e.g., Form is rate-limited and doesn't expose backend systems).

301-12 Manage Remote Access (AC-17)

Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and authorize each type of remote access to the system prior to allowing such connections.

AC-17(1): Employ automated mechanisms to monitor and control remote access methods especially in cloud environments, for connectivity for unauthorized use.

AC-17(2): Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions following a multi-layer ZTA approach such as identity-based authentication and dynamic authorization, granular access controls, and software-defined perimeters. When administrative actions are performed from external connections, the use of an encrypted remote connection is required using robust encryption. Minimum encryption standards are defined in MD-STD-318-SC, Section 318-6.

AC-17(3): Route remote access through authorized and managed network access control points.

AC-17(4): Authorize the execution of privileged commands and access to security-relevant information via remote access only if approved by the appropriate AO and in a format that provides assessable evidence and for compelling operational needs. Document the rationale for remote access, log/record sessions, and monitor via centralized logging (e.g., PAM tools).

301-13 Manage Wireless Access (AC-18)

Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access, and authorize each type of wireless access to the system prior to allowing such connections.

Configuration and connection requirements include at a minimum:

- Guest users accessing guest wireless networks must be registered through a captive portal.
- Cryptographic solutions must meet minimum encryption standards as defined in MD-STD-318-SC, Section 318-6;
- Connectivity to wireless networks must use security protocols that provide mutual authentication, verifying both the device and the network, such as Extensible Authentication Protocol–Transport Layer Security (EAP-TLS);
- Management connectivity to the wireless infrastructure shall be segregated from user connectivity;
- Physical or logical separation between guest/public networks and employee/secure networks;
- Event logging to a centralized log management server;
- Each type of wireless access to the system shall be authorized prior to allowing such connections; and
- Where feasible, wireless intrusion detection/prevention (WIDS/WIPS) technology should be used.

AC-18(1): Protect wireless access to the system using authentication of both users and devices and encryption that meets the minimum encryption standards defined in MD-STD-318-SC, Section 318-6.

AC-18(3): When not intended for use, disable wireless networking capabilities embedded within system components prior to issuance and deployment.

301-14 Manage Mobile Devices (AC-19)

State mobile devices (e.g., smartphones, tablets, and other portable endpoints running iOS, Android, or Google-managed platforms) issued by the agency must be actively managed using a Mobile Device Management (MDM) platform in accordance with agency procedures to include at a minimum:

- Automated provisioning of devices with necessary configurations;
- Enforcement of agency-defined security policies for devices;
- Implementation of device encryption and data protection (e.g., passcode policies, biometric authentication);
- Deployment, update, and removal of applications centrally (e.g., over-the-air (OTA) updates);
- Geolocation tracking, geofencing and location-based controls;
- Integration with identity management systems;
- Remote wipe and lock;
- Audit trail and logging; and
- Application whitelisting and blacklisting.

Contractors may be issued State mobile devices at the discretion of the issuing agency, as business needs necessitate, to minimize exposure of State data among non-State devices.

Personally owned devices shall not access, store, transmit, or process State non-public data (Data Classification Level 2 or above) unless explicitly authorized by the designated agency official (e.g., AO or equivalent). Such authorization shall be granted only when the device meets the minimum technical safeguards approved by OSM. Where required technical safeguards cannot be applied to the personally owned device, but the agency official elects to authorize use, the State data being accessed shall be limited to data types approved by the agency and shall be protected by technical controls that prevent data export, including but not limited to downloading, saving, or transferring State data outside of approved systems.

Contractor-owned devices shall not access, store, transmit, or process State data unless explicitly authorized by the contract; and the device meets the minimum technical safeguards defined in the contract.

AC-19(5): Employ full-device encryption to protect the confidentiality and integrity of information on mobile devices. Minimum encryption standards are defined in MD-STD-318-SC, Section 318-6.

301-15 Manage the Use of External Systems (AC-20)

Restrict access to all external information systems unless explicitly authorized by the agency AO consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing only authorized individuals to:

- Access the system from external systems; and
- Process, store, or transmit organization-controlled information using external systems.

External Information Systems

External information systems in the context of the MD policy and standards include, but are not limited to: a) Personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); b) Privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); c) Information systems owned or controlled by non-State governmental organizations; and d) State information systems that are not owned by, operated by, or under the direct supervision and authority of the Executive Branch.

AC-20(1) Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

- Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans;
- Retention of approved system connection or processing agreements with the organizational entity hosting the external system; and
- Approval from the agency privacy officer (or State Chief Privacy Officer).

AC-20(2): Restrict the use of agency-controlled portable storage devices by authorized individuals on external systems to those with a business need, and require any storage media containing non-public data (Data Classification Level 2 or above) by the data owner to be encrypted, and at all times be stored securely, until such time as the storage media has been sanitized in a manner consistent with the classification of the data.

301-16 Control Information Sharing (AC-21)

Enable authorized users to determine whether access authorizations assigned to a sharing partner (i.e., any external entity with whom an agency exchanges information) match the information's access and use restrictions for non-public State data (Data Classification Level 2 and above) as contractually obligated; and employ automated or manual processes to assist users in making information sharing and collaboration decisions.

Example use cases include: a) State users accessing data hosted by a cloud vendor; b) Vendor accessing State data/systems; and c) Application (non-human) accounts accessing data hosted outside the State and vice versa.

301-17 Manage Publicly Accessible Content (AC-22)

Designate agency individuals authorized to make information publicly accessible; Train authorized individuals to ensure that publicly accessible information does not contain non-public information (Data Classification Level 2 or above); Review the proposed content prior to posting onto the publicly accessible system to verify that non-public information is not included; and Review the content on the publicly accessible system for non-public information at least **quarterly** and remove such information, if discovered.

GUIDELINES

ID	Title	Description	Source
CSF Tools	Cybersecurity Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools* *(LINK)*
NIST SP 800-162	Guide to Attribute-Based Access Control (ABAC)	This document defines ABAC and provides considerations for its implementation.	*csrc.nist.gov* *(LINK)*
NIST SP 800-192	Verification and Test Methods for Access Control Policies/Models	This publication focuses on verifying and testing access control policies to verify correctness and security.	*csrc.nist.gov* *(LINK)*
NIST SP 800-207	Zero Trust Architecture	This document is a foundational publication for Zero Trust Architecture.	*csrc.nist.gov* *(LINK)*

DEFINITIONS

Each unique term used in this standard is defined in the **State of Maryland Cybersecurity & Privacy Glossary**.

COMPLIANCE CHECKLIST

ID	Standard	Compliance
301-1	Develop Agency-Level Procedures (AC-1)	☐ Yes ☐ No
301-2	Manage System Accounts (AC-2)	☐ Yes ☐ No
301-3	Enforce Authorized Access (AC-3)	☐ Yes ☐ No
301-4	Control the Flow of Information (AC-4)	☐ Yes ☐ No
301-5	Maintain Separation of Duties (AC-5)	☐ Yes ☐ No
301-6	Employ the Principle of Least Privilege (AC-6)	☐ Yes ☐ No
301-7	Enforce Limits on Unsuccessful Logon Attempts (AC-7)	☐ Yes ☐ No
301-8	System Use Notification (AC-8)	☐ Yes ☐ No
301-9	Require Device Lock (AC-11)	☐ Yes ☐ No
301-10	Automatically Terminate Sessions (AC-12)	☐ Yes ☐ No
301-11	Identify all System Actions Permitted Without Identification or Authentication (AC-14)	☐ Yes ☐ No
301-12	Manage Remote Access (AC-17)	☐ Yes ☐ No
301-13	Manage Wireless Access (AC-18)	☐ Yes ☐ No
301-14	Manage Mobile Devices (AC-19)	☐ Yes ☐ No
301-15	Manage the Use of External Systems (AC-20)	☐ Yes ☐ No
301-16	Control Information Sharing (AC-21)	☐ Yes ☐ No
301-17	Manage Publicly Accessible Content (AC-22)	☐ Yes ☐ No

Note: When assessing the implementation and effectiveness of the security and privacy controls outlined in this standard, DoIT recommends the use of NIST SP 800-53A Rev. 5, to perform evaluations in a manner that is evidence-based, repeatable, and aligned with the system’s documented security posture.