Maryland
STATE DEPARTMENT OF EDUCATION

CYBERSECURITY POLICY

ACCESS CONTROL

Office of Information Technology, Chief Information Security Officer

June 2024

Document Control

Title:	Cybersecurity Policy - Access Control
Security Level:	Non-sensitive
File Name:	Access Control.pdf

Document History

Document Version	Date	Summary of Change
1.0	June 2024	Initial Document, Cancels Agency Directive AD 21201-002

RECORD OF CHANGES

The Document Version details changes made to the policy outside the official policy maintenance and review cycle. Annual Reviews shall be annotated In Document History or released under a whole number version (1.0, 2.0, 3.0, ...) for a major revision.

APPROVALS

This Cybersecurity Policy was prepared by the MSDE to develop, implement, and maintain a resilient and secure cyberspace for the Department. This policy is consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

Approved: Shawn Fritz-Rushing Date Sep 24, 2024

Shawn Rushing

Assistant State Superintendent of Operations and Administration

Submitted: Date Sep 18, 2024

Andrew Neboshynsky

Chief Information Security Officer

Table of Contents

Introduction

Maryland State Department of Education has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its data. These policies are set forth by Maryland State Department of Education’s management and in compliance with the Access Control family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

Purpose

These policies establish access control requirements to ensure the confidentiality, integrity, and availability of Maryland State Department of Education’s systems, facilities, and data. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

This policy cancels Maryland State Department of Education Agency Directive AD 21201-002: Access Control for Information and Information Systems.

Scope

The provisions of these policies pertain to all Maryland State Department of Education employees, contractors, third parties, and others who have access to company and customer confidential information within Maryland State Department of Education systems and facilities.

Roles and Responsibilities

These policies apply to all Maryland State Department of Education employees, contractors, business partners, third parties, and others who need or have access to Maryland State Department of Education’s systems and our customer's confidential information.

Individual or Group	Role	Responsibility
Krishnanda Tallur	Deputy State Superintendent for Operations and Finance	Responsible for developing, implementing, maintaining, and ensuring compliance with Cybersecurity policies, procedures, and controls. Has final responsibility for Cybersecurity program.
Shawn Fritz-Rushing	Assistant State Superintendent for Administration and Operations	Responsible for developing, implementing, maintaining, and ensuring compliance with Cybersecurity policies, procedures, and controls. Has final responsibility for Cybersecurity program.
Vacant	Information Owner/ Data Governance Officer	Has statutory, management, or operational authority for Maryland State Department of Information's information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal.
Shawn Fritz-Rushing	Authorizing Official/ Chief Information Officer	Responsible for operating information system at an acceptable level of risk to organizational operations and assets.
Andrew Neboshynsky	Authorizing Official Designated Representative	Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process.
Andrew Neboshynsky	Chief Information Security Officer	Responsible for conducting information system security engineering activities. Responsible for providing appropriate security, including management, operational, and technical controls.

Ian Goodhart	Information System Security Officer	Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures.
System Admin Team	System Administrator	Responsible for conducting information system security Administration activities.
Varies	Managers	Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures.
Varies	Users	Responsible for understanding and complying with Policies and Procedures.

Management Commitment

Maryland State Department of Education and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the Maryland State Department of Education Information Systems by implementing adequate security controls.

Authority

These policies and procedures are issued under the authority of the Maryland State Department of Education Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)

7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011
10. The State of Maryland Information Technology Security Manual v1.2

Compliance

Compliance with these policies is mandatory. It is Maryland State Department of Education's policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed by an external vendor and/or internal self-assessments to identify areas of non-compliance. Any findings identified in the audit will be remediated, either through mitigation, removal, or risk acceptance waivers for vulnerabilities that cannot be sufficiently mitigated.

Policy Requirements

The following personally identifiable information processing and transparency controls requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support information systems owned and operated by Maryland State Department of Education, including its subsidiaries and affiliates, collectively referred to as MSDE.

The following access control requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support MSDE information systems.

ACCESS CONTROL POLICIES AND PROCEDURES [AC-1]

This document is intended to serve as the Access Control Policy and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the Access Control Policy and related controls have been developed, documented, and disseminated to all applicable personnel.

Maryland State Department of Education must develop, document, and disseminate to all personnel including the Chief Privacy Officer, ISSO, and/or similar roles or their designees: [AC-1 (a)]

- An organizational-level Access Control Policy that: [AC-1 (a) (1)]

  - Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance [AC-1 (a) (1) (a)]
  - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines [AC-1 (a) (1) (b)]
- Procedures to facilitate the implementation of Access Control Policy and the associated Access Control controls [AC-1 (a) (2)]

Maryland State Department of Education must designate a Chief Information Security Officer (CISO) to manage the development, documentation, and dissemination of the Access Control policy and procedures. [AC-1 (b)]

Maryland State Department of Education must review and update the current Access Control: [AC-1 (c)]

- Policies at least annually, following a significant change, and/or any compromising event [AC-1 (c) (1)]
- Procedures at least annually, following a significant change, and/or any compromising event [AC-1 (c) (2)]

ACCOUNT MANAGEMENT [AC-2, AC-2 (1,2,3,4,5,7,9,12,13), {AC-2 (11) HIGH ONLY}]

Maryland State Department of Education has implemented and maintains an information system account management process intended to carry out the following activities: [AC-2]

- Identify and document accounts necessary to support company mission and business functions including Individual, Group, System, Application, Guest/Anonymous, Temporary, and other accounts if they exist [AC-2 (a)]
- Assign account managers for information system accounts [AC-2 (b)]
- Establish conditions for group and role membership [AC-2 (c)]
- Specify:
  - Authorized users of the system, [AC-2 (d) (1)]
  - Group and role membership, [AC-2 (d) (2)]
  - Access authorizations, and defined attributes for each account [AC-2 (d) (3)]
- Ensure all information system accounts require approval by defined personnel or roles [AC-2 (e)]
- Maintain the capability to establish, activate, modify, disable, or remove accounts in accordance with defined policies and procedures [AC-2 (f)]
- Monitor information system account users [AC-2 (g)]
- Ensure mechanisms are implemented to notify account managers within
  - Twenty-four (24) hours when accounts are no longer required, [AC-2 (h) (1)]
  - Eight (8) hours when information system users are terminated, transferred, or [AC-2 (h) (2)]

  - Eight (8) hours when information system usage or need-to know/need-to-share changes [AC-2 (h) (3)]
- Grant information system access based on a valid access authorization, job/role requirements, intended system usage, and other product specific attributes [AC-2 (i)]
- Review accounts for compliance with account management requirements [AC-2 (j)]
  - Monthly for privileged accessed and every six (6) months for non-privileged access for high impact systems
  - Quarterly for privileged access and annually for non-privileged access for all other systems
- Employ a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group [AC-2 (k)]
- Align account management processes with personnel termination and transfer processes [AC-2 (l)]

Additionally, Maryland State Department of Education must:

- Support the management of system accounts using automated mechanisms to alert system administrators when personnel have been hired or terminated [AC-2 (1)]
- Have mechanisms in place to automatically remove or disable temporary and emergency accounts after no more than no more than 24 hours from last user use for high impact system and no more than 96 hours from last use for all others [AC-2 (2)]
- Disable accounts within 24 hours for user accounts: [AC-2 (3)]
  - After account has expired [AC-2 (3) (a)]
  - Are no longer associated with a user or individual [AC-2 (3) (b)]
  - Are in violation of organizational policy [AC-2 (3) (c)]
  - Have been inactive for thirty-five (35) days for high impact systems or ninety (90) days for all others [AC-2 (3) (d)]
- Automatically audit account creations, privileged group membership modifications, and disabling and terminating actions [AC-2 (4)]
- Require users to log out at the end of use's standard work period for all systems and if inactivity is anticipated to exceed fifteen (15) minutes for high impact systems [AC-2 (5)]
- Establish and administer privileged user accounts in accordance with a role-based access scheme [AC-2 (7) (a)]
- Monitor all privileged role assignments [AC-2 (7) (b)]
- Monitor all changes to roles or attributes [AC-2 (7) (c)]
- Take action to revoke access when privileged role or attribute assignments are no longer appropriate [AC-2 (7) (d)]
- Require that organization defined conditions be met to permit the use of shared or group accounts with justification statement that explains why such accounts are necessary [AC-2 (9)]

- Monitor system accounts for escalation of privileges, unauthorized tenant access, and report atypical usage changes to data fields to the ISSO and/or similar role [AC-2 (12)]
- Disable accounts of individuals within one (1) hour of discovery of activities that have adverse impacts to organizational operations, organizational assets, individuals, other entities. [AC-2 (13)]

For high impact systems only:

- Maryland State Department of Education must establish and enforce the specific conditions or circumstances under which system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time. [AC-2 (11)]

ACCESS ENFORCEMENT [AC-3]

Maryland State Department of Education must enforce approved authorizations for logical access to information and system resources in accordance with applicable Maryland State Department of Education defined, identity-based, role-based, attribute-based policies and procedures.

INFORMATION FLOW ENFORCEMENT [AC-4, AC-4 (21), {AC-4 (4) HIGH ONLY}]

The Maryland State Department of Education Cybersecurity team enforces approved authorizations for controlling the flow of information within the system and between interconnected systems. Acceptable information flow is based on application tiers, subnet functions, and instance purpose. [AC-4]

Maryland State Department of Education information systems separate the information flow logically or physically using VNets, Subnets, NSGs, and firewalls to accomplish separation of Application tiers, subnet functions, and instance purposes. [AC-4 (21)]

For high impact systems only:

Maryland State Department of Education must prevent encrypted information from bypassing intrusion detection mechanisms by

- decrypting the information;
- blocking the flow of the encrypted information; or
- terminating communications sessions attempting to pass encrypted information. [AC-4 (4)]

SEPARATION OF DUTIES [AC-5]

Maryland State Department of Education maintains a separation of duties matrix for privileged and non-privileged user roles. The matrix has been documented and implemented across the organization in order to define the duties of individual employees, prevent malicious activity without collusion, and assign information system access authorizations. The separation of duties matrix shall be disseminated using the OIT Operations site.

LEAST PRIVILEGE [AC-6, AC-6 (1,2,5,7,9,10), {AC-6 (3,8) HIGH ONLY}]

Maryland State Department of Education must follow the least privileged concept. Only the minimum necessary system privileges required to perform job duties are granted to an individual. [AC-6]

The following measures have been put in place to ensure compliance with the least privilege requirements:

- Explicit authorization must be granted through the account authorization process to receive access to the environment hosting Maryland State Department of Education applications and any security product or security information supporting those applications. [AC-6 (1)]
- Individuals with access to all security functions are required to use a unique, non-privileged account when performing non-administrative functions. [AC-6 (2)]
- Privileged accounts on the information system are restricted to defined personnel or roles whose job functions require privileged access. [AC-6 (5)]
- Review, at a minimum, annually the privileges assigned to all privileged users to validate the need for such privileges and, if necessary, reassign or remove privileges to correctly reflect organizational mission and business needs. [AC-6 (7)]
- Information systems are configured to log and support the audit of execution of privileged functions. [AC-6 (9)]
- Non-privileged users are prevented from executing privileged functions including disabling, circumventing, or altering implemented security safeguards or countermeasures. [AC-6 (10)]

For high impact systems only:

- Authorize network access to all privileged commands only for operational needed and document the rationale for such access in the security plan for the system. [AC-6 (3)]
- Prevent any software from executing at higher privilege levels than users executing any software except software explicitly documented. [AC-6 (8)]

UNSUCCESSFUL LOGON ATTEMPTS [AC-7]

Users must be limited to three (3) consecutive invalid logon attempts during a fifteen (15) minute time period. If the user exceeds the maximum number of unsuccessful logon attempts, the account/node must be automatically locked for thirty (30) minutes.

SYSTEM USE NOTIFICATION [AC-8]

Maryland State Department of Education information systems are configured to display a System Use Notification Banner when users access the information system. [AC-8] Additionally, Maryland State Department of Education information systems retain the notification message or banner on the screen prior to granting access to the information system. [AC-8 (b)]

The system use notification must include the following information [AC-8 (a)]:

- Users are accessing a government or corporate information system, where appropriate
- System usage may be monitored, recorded, and subject to audit
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties
- Use of the system indicates consent to the monitoring and recording
- Publicly accessible systems display the following information [AC-8 (c)]:
- System use information when appropriate, before granting further access
- References, if applicable, to monitoring, recording, or auditing, that are consistent with privacy
- accommodations for such systems that generally prohibit those activities
- A description of authorized usage

CONCURRENT SESSION CONTROL [AC-10 {HIGH ONLY}]

For high impact systems only:

Maryland State Department of Education must limit the number of concurrent sessions for privileged users to no more than three (3) sessions and no more than two (2) sessions for non-privileged users per target device.

DEVICE LOCK [AC-11, AC-11 (1)]

Maryland State Department of Education information systems must have a session lock that is triggered after no more than fifteen (15) minutes of inactivity or upon receiving a user request. Maryland State Department of Education requires users to initiate a device lock before leaving their system unattended. The system must retain the session lock until the user re-established access using their authentication credentials. [AC-11]

Maryland State Department of Education must configure terminals so that information previously visible on the display is concealed with a publicly viewable image upon activation of a session lock. [AC-11 (1)]

SESSION TERMINATION [AC-12]

User sessions must be automatically terminated after receiving a logout request from either the user or the application. User sessions may also be automatically terminated after trigger events occur, such as periods of user inactivity, machine shutdown/reboot requests, or time-of-day restrictions on system use. [AC-12]

PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION [AC-14]

Maryland State Department of Education must restrict user actions that can be performed on information systems without identification or authentication to (i) viewing logon prompts and the warning banner or (ii) initiating an out of band password reset on systems that require authentication. Maryland State Department of Education must document and provide supporting rationale in the security plan for user actions not requiring identification or authentication. For the avoidance of doubt, this requirement does not apply to publicly available content (i.e. Marketing websites).

REMOTE ACCESS [AC-17, AC-17 (1,2,3,4)]

Maryland State Department of Education must establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access permitted. Each type of remote access to an information system must be authorized prior to allowing such connections. [AC-17]

Maryland State Department of Education must monitor and control remote access methods. [AC-17 (1)] Cryptographic mechanisms must be implemented to protect the confidentiality and integrity of remote access sessions. [AC-17 (2)] All remote access must be routed through a limited number of authorized and managed network access control points. [AC-17 (3)]

Execution of privileged commands and access to security-relevant information via remote access are only authorized for web application or production environment support, and the rationale for providing authorization must be documented in the System Security Plan. [AC-17 (4)] Termination of any unauthorized remote access connections to the system shall be initiated within fifteen (15) minutes of discovery.

WIRELESS ACCESS [AC-18, AC-18 (1,3), {AC-18 (4,5) HIGH ONLY}]

Maryland State Department of Education must:

- Establish configuration requirements, connection requirements, and implementation guidance prior to allowing and authorizing each type of wireless access connections [AC-18]
- Protect wireless access to the system using authentication at the device level along with encryption [AC-18 (1)]
- Ensure embedded wireless networking capabilities are disabled prior to issuance and deployment when such capabilities not intended for use [AC-18 (3)]

For high impact systems only:

- Explicitly identify and authorize users that are allowed to independently identify and configure wireless networking capabilities [AC-18 (4)]

- Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries [AC-18 (5)]

ACCESS CONTROL FOR MOBILE DEVICES [AC-19, AC-19 (5)]

Maryland State Department of Education has implemented usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices. [AC-19 (a)] All mobile device connections must be authorized prior to use and only if they meet established usage restrictions. [AC-19 (b)]

Full-device encryption and/or container encryption must be implemented prior to device issuance to protect the confidentiality and integrity of the information on mobile devices. [AC-19 (5)]

USE OF EXTERNAL SYSTEMS [AC-20, AC-20 (1,2)]

Where applicable, Maryland State Department of Education shall establish terms and conditions and identify required controls to be implemented on external systems before allowing authorized individuals to process, store, and/or transmit data between Maryland State Department of Education controlled information systems and external information systems. This may be documented in the Terms and Conditions of the agreement between Maryland State Department of Education and the external information system provider. [AC-20 (a)]

Maryland State Department of Education prohibits accessing the information system from embargoed countries and countries known for state sponsored cyber threats. Maryland State Department of Education prohibits the processing, storing, or transmitting of Maryland state data on systems geolocated outside the United States. [AC-20 (b)]

Maryland State Department of Education permits authorized individuals to use an external information system to access Maryland State Department of Education systems or to process, store, or transmit organization-controlled information only after [AC-20 (1)]:

- The implementation of required security controls have been verified on the external information system, in accordance with the Maryland State Department of Education Cybersecurity policies and security plans [AC-20 (1) (a)]; or
- Retention of approved system connection or processing agreements with the organizational entity hosting the external system. [AC-20 (1) (b)]

The use of Maryland State Department of Education controlled portable storage devices by authorized individuals on external information systems is prohibited without explicit authorization from the Maryland State Superintendent of Schools or delegate. [AC-20 (2)]

INFORMATION SHARING [AC-21]

To facilitate information sharing, Maryland State Department of Education authorized Cybersecurity leadership with the ability to determine whether access authorizations assigned to the sharing partner match the access and use restrictions on the information being shared and with noting circumstances where user discretion is required. [AC-21 (a)]

Additionally, Maryland State Department of Education must employ automated mechanisms and manual processes to assist users in making information sharing/collaboration decisions. [AC-21 (b)]

PUBLICLY ACCESSIBLE CONTENT [AC-22]

Only designated and authorized individuals are permitted to post publicly accessible information onto an information system. [AC-22 (a)] All authorized individuals must be trained to ensure that publicly accessible information does not contain non-public information. [AC-22 (b)]

All content must be reviewed by the Office of Communications and Community Engagement for non-public information before it is posted onto any Maryland State Department of Education information system as publicly accessible. [AC-22 (c)] All information publicly published must be reviewed for non-public information at least quarterly and any such non-public information must be removed from public view. [AC-22 (d)] Discovery of the public publishing of any non-public information must be reported to the Office of Communications and Community Engagement for investigation.